SOPHOS

Sophos Enterprise Console

帮助

产品版本：4.5

文档日期：2010 年 6 月



目录

1 关于 Sophos Enterprise Console

Sophos Enterprise Console 版本 4.5，是独立的，自动化的控制台，它统一部署和管理 Windows，Mac，Linux，和 UNIX 计算机上的 Sophos 安全软件。Enterprise Console 使您能够：

- 保护您的网络免遭病毒，特洛伊木马，蠕虫，间谍软件，恶意网站，以及未知的安全隐患的侵害，同时，还防范广告软件和其它可能不想安装的应用程序。
- 控制哪些应用程序可以在网络中运行。
- 管理终结点计算机上的客户端防火墙保护。
- 在计算机被允许登录到网络中，以及强制实施遵照之前，根据您设置的条件，评估计算机的遵照状况。
- 减少从终结点计算机意外丢失数据，例如：无意中传输的敏感数据。
- 防止用户在终结点计算机上使用未经批准的外部存储设备和无线网络连接技术。
- 防止用户重新配置，禁用，或者，卸载 Sophos 安全软件。

如果您是首次使用 Enterprise Console，请参见 开始使用（第9页）。

2 Enterprise Console 简介

2.1 关于界面

您可以通过 Sophos Enterprise Console 界面使用和配置使用 Sophos 安全软件。它的主要功能说明如下。

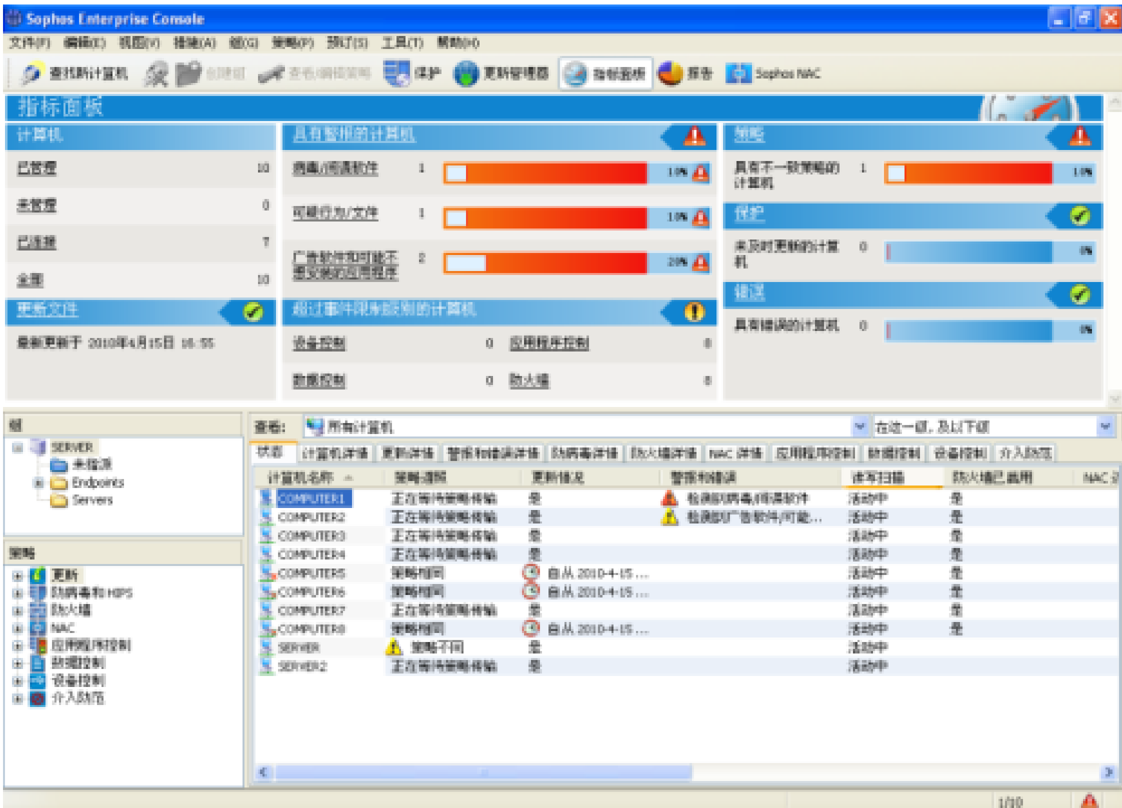


图1：Enterprise Console - 终结点视图

指标面板

指标面板提供网络安全状态的“一览图”。要显示或隐藏指标面板，请单击工具栏上的 **指标面板** 按钮。要了解更多有关“指标面板”的信息，请参见 指标面板概述（第45页）。

计算机列表

计算机列表（右手边的窗格板）具有两个视图：**终结点** 视图和 **更新管理器** 视图。您可以通过单击工具栏上的 **更新管理器** 或 **终结点** 按钮，在两个试图之间切换。

终结点 视图显示所选择的组中的终结点计算机。此视图由数个标签页组成。**状态** 标签页，显示计算机是否受到读写扫描的保护，它们是否遵照各自的组策略，那些功能处于启用状态，以及软件是否已及时更新。此标签页还显示是否有任何警报发出。其它的标签页会就不同的主题给出更详细的信息。

要了解显示在计算机列表中的图标的含义，请参见。图标的含义（第8页）

您可以在 **终结点** 视图中复制或打印显示在计算机列表中的信息。要了解更多信息，请参见“从 Enterprise Console 复制和打印数据”部分。

更新管理器 视图中会显示安装了 Sophos Update Manager 的计算机。在此视图中，您可以设置自动从 Sophos 网站更新 Sophos 安全软件，并查看各更新管理器的状态和详情。



图2：**Enterprise Console - 更新管理器视图**

组窗格板

组 窗格板会在选择 **终结点** 视图时出现。在 **组** 窗格板中，您可以创建，并将联网计算机放置其中。您可以自己创建组，也可以从 Active Directory 容器中导入组（所导入的组可以包含计算机，也可以不包含计算机。），并将这些组用作为 Enterprise Console 计算机组。

未指派 组 用于尚未指派给组的计算机。要配置组，请选择它并单击右键。

策略窗格板

策略 窗格板会在选择 **终结点** 视图时出现。在 **策略** 窗格板中，您可以创建或更改应用到计算机组中的策略。要配置策略，请选择它并单击右键。

软件预订窗格板

软件预订 窗格板会在选择 **更新管理器** 视图时出现。在 **软件预订** 窗格板中，您可以创建或编辑软件预订，指定为在何种操作系统上使用的 Sophos 下载哪个版本的终结点计算机软件。

工具栏

查找新计算机 可以搜索网络中的计算机，并将它们添加到控制台中。

创建组 为计算机创建新组。

查看/编辑策略 使您能够打开和更改在 **策略** 窗格板中选择的策略。

保护 使您能够在从计算机列表中选择的计算机上安装防病毒和防火墙软件。

更新管理器/终结点 在计算机列表窗格板中显示的视图之间切换。

报告 使您能够生成有关您的网络中的警报和事件的报告。

指标面板 可以打开指标面板，它提供了网络安全状态的“一览图”。

Sophos NAC 可以打开 Sophos NAC Manager，您可以用它来编辑 NAC（网络访问控制）策略。

2.2 什么是组？

组是放置数个计算机的一个文件夹。

您可以自己创建组，也可以从 Active Directory 容器中导入组（所导入的组可以包含计算机，也可以不包含计算机。），并将这些组用作为 Enterprise Console 计算机组。您还可以设置与 Active Directory 同步化，这样在 Active Directory 中新添的计算机和容器，以及其它更改都会被自动复制到 Enterprise Console 中。

各个组都有针对更新，防病毒和 HIPS 保护，防火墙保护，等等的设置。在组中的所有计算机应该通常使用这些设置，它们被称为“策略”。

组可以包含子组。

2.3 什么是策略？

策略是应用到组中的所有计算机的设置的集合。

当您安装 Enterprise Console 时，安装过程会为您创建默认的策略，提供基本的安全保护。这些策略会应用到您创建的任何组。您可以编辑默认策略，或者，创建新的策略。

要了解更多有关不同类型的策略的信息，请参见策略是干什么的？（第24页）。

2.4 什么是未指派组？

未指派 组是 Enterprise Console 放置尚未放置到组中的计算机的文件夹。

您不能：

- 应用策略到 **未指派** 组。
- 在 **未指派** 组中创建子组。
- 移动或删除 **未指派** 组。

2.5 图标的含义

在计算机列表的 **终结点** 视图里，所使用的图标含义:

- 警报
- 保护被禁用，或者没有及时更新。
- 每台计算机的状态，如：软件是否正在被安装。

警报

图标	释意
	出现在 **状态** 标签页里的 **警报和错误** 栏中的红色警报标志表明，检测到了病毒，蠕虫，特洛伊，间谍软件，或可疑行为。
	出现在 **状态** 标签页里的 **警报和错误** 栏中的黄色警告标志表明，以下情况之一: ■ 检测到了可疑文件。 ■ 检测到了广告软件或其它可能不想安装的应用程序。 ■ 出现错误。 出现在**策略遵照**栏中的黄色警告标志表明，该计算机没有使用与它所在的组中的其它计算机使用的策略相同的策略。

如果计算机中出现了多个警报和错误，具有最高的优先级的警报的图标，会出现 **警报和错误** 栏中。以下列示的警报类型，以降序排列优先级。

1. 病毒和间谍软件警报
2. 可疑行为警报
3. 可疑文件警报
4. 广告软件和可能不想安装的应用程序 (PUA) 警报
5. 软件应用程序错误（例如，安装错误）

保护被禁用，或者没有及时更新。

图标	释意
	灰色的盾牌说明读写扫描处于没有激活状态。
	灰色防火墙标志说明防火墙处于禁用的状态。
	时钟图标说明所使用的软件没有及时更新。

计算机状态

图标	释意
	蓝色的计算机标识说明，该计算机已被 Enterprise Console 管理。
	带有黄色箭头的计算机标识说明，防病毒软件和防火墙软件的安装处于等待状态。
	带有绿色箭头的计算机标识说明，软件的安装正在进行中。
	带有沙漏的计算机标识说明，终结点安全软件的自动更新组件已安装，并且正在下载软件的最新版本。
	灰色的计算机标志说明，该计算机未被 Enterprise Console 管理。
	旁边带有红色叉的计算机标识表明，该通常受 Enterprise Console 管理的该计算机已经断开了与网络的连接。（没有被管理的与网络断开了连接的计算机，不会被显示。）

3 开始使用

这是在您安装了 Enterprise Console 和完成了 **下载安全软件向导** 之后，需要执行的，以保护您的网络的任务的概览。要了解更多有关使用 Enterprise Console 的信息，请参见提及的其它材料和章节。

Sophos 建议您参见 *Sophos Endpoint Security and Control* 策略设置指南，寻求有关使用和管理 Sophos 安全软件的最佳使用方式的建议。Sophos 技术文档发布在 *http://cn.sophos.com/support/docs/* 中。

如果您尚未完成 **下载安全软件指南**，请参见 运行下载安全软件向导（第 66页）。

要保护您的网络，请按照以下步骤做：

1. 创建组。

   您可以自己一个一个地创建组，也可以从Active Directory容器中导入组（所导入的组可以包含计算机，也可以不包含计算机。），并将这些组用作为Enterprise Console 计算机组。

   如果您想要导入Active Directory 容器，请参见 *从 Active Directory 中导入容器和计算机*（第30页）。Sophos 建议首先导入没有计算机的 Active Directory 容器，然后，指定组策略到组中，然后添加计算机到组中，例如，通过同步化 Active Directory 计算机的方式。

   要了解有关手动创建组的信息，请参见"创建和使用组"部分。

2. 设置策略。

   Enterprise Console 具有一组默认的策略，它们对保护您的网络非常重要。您可以立即就使用默认的 **更新** 和 **防病毒和 HIPS** 策略。您必须通过运行 **防火墙策略** 向导来配置防火墙策略。请参见 设置防火墙（第110页）。

3. 查找网络中德计算机，并将它们添加到控制台。

   如果您已经在步骤1中导入了 Active Directory 容器和计算机，那么，您需要进行任何操作。否则，请参见"查找网络中的计算机"部分。

4. 保护计算机。

   根据最适合您的情况，您可以在以下二种方法中选择保护联网计算机的方式。

   - **使用保护计算机向导**

     当您从 **未指派** 组中将计算机拖放到其它组中时，会有一个向导启动，帮助您保护计算机。请参见"保护新的计算机"部分。

   - **在与 Active Directory 同步化时自动保护计算机**

     如果您选择了与 Active Directory 同步化，您还可以选择自动保护 Windows 2000 或以后的计算机。您可以在 **与 Active Directory 同步化向导** 中，或者在 **同步化属性** 对话框中，这样做。要了解操作指导，请参见 使用同步化自动保护计算机（第38页）。

5. 检查计算机是否受到保护

   当安装完成时，再次查看在新组中的计算机列表。在 **读写扫描** 栏中，您应该看到"活动"字样：这表明计算机已受到读写扫描的保护，受到 Enterprise Console 的管理。要了解更多信息，请参见 怎样检查网络是否受到保护？（第44页）。

6. 清除计算机。

   如果在您的网络中检测到了病毒，不想安装的应用程序，或其他项目，或可能不想安装的应用程序，请按照“清除计算机”部分中的说明，清除受影响的计算机。

附加的保护和管理选项

依照默认值，Sophos Endpoint Security and Control 会检测病毒，特洛伊木马，蠕虫，以及间谍软件。Windows 2000 及以后的计算机上的 Sophos Anti-Virus 7 及以后，还可以分析在系统中运行的程序的行为。您可以添加更多的保护措施，例如，防范广告软件，其它可能不想安装的应用程序 (PUAs)，可疑或不想要的行为，或者，从工作站计算机上意外丢失数据。参见以下章节了解更多的信息:

- 关于防病毒和 *HIPS* 策略（第77页）
- 设置防火墙（第110页）
- 关于应用程序控制（第120页）
- 关于数据控制（第123页）
- 关于设备控制（第138页）
- 关于 *NAC*（第145页）
- 关于介入防范（第148页）

您可以在 Enterprise Console 中设置不同的角色，添加权限到角色中，然后指派 Windows 用户和组到角色中。包括了 Sophos Full Administrators Windows 组的 System Administrator 角色具有完全的权限，不需要设置。要了解更多有关角色的信息，请参见“管理角色和子领域”部分。

您可以将 IT 领域分成多个子领域，并将 Enterprise Console 的计算机组指派给这些子领域。这样您可以通过指派 Windows 用户和组给子领域，从而控制对子领域的访问。 **默认** 子领域包含包括 **未指派** 组在内的所有 Enterprise Console 组。要了解更多有关子领域的信息，请参见“管理角色和子领域”部分。

4 管理角色和子领域

4.1 关于角色和子领域

重要: 如果您已使用基于角色的管理，您必须具有 **基于角色的管理** 权限，才能设置角色和子领域。包括了 Sophos Full Administrators Windows 组的 System Administrator 角色具有完全的权限，不需要设置。要了解更多信息，请参见什么是预设的角色？（第13页）和 。各种权限有权处理什么任务？（第17页）

通过设置角色，添加权限到该角色，然后，指派Windows用户和组到角色中，您可以设置基于角色的控制台访问。例如，提供桌面支持的工程师可以更新或清除计算机，但是，不能配置策略 — 这是系统管理员所负责的工作。

要开启 Enterprise Console，用户必须是 Sophos Console Administrators 组的成员，并且至少被指派给一个 Enterprise Console 角色和一个子领域。Sophos Full Administrators 组的成员具备完全访问 Enterprise Console 的权限。

注: 如果您想允许用户使用远程的或附加的 Enterprise Console，请参见 别的用户怎样使用 *Enterprise Console?* （第171页）。

您可以创建自己的角色，也可以使用预设的角色。

您可以指派某用户为各种角色，方法是添加该单个的用户或添加该用户所属的 Windows 组到各种角色中。

如果某用户没有在控制台中执行某特定任务的权限，他们仍然可以在只读模式中查看相关任务的配置设置。您指派给任何角色的用户，将无法打开 Enterprise Console。

您还可以限制用户在某些计算机和计算机组中执行操作。您可以将 IT 领域分成多个子领域，并将 Enterprise Console 的计算机组指派给这些子领域。这样您可以通过指派 Windows 用户和组给子领域，从而控制对子领域的访问。 **默认**子领域包含包括 **未指派** 组在内的所有 Enterprise Console 组。

用户只能查看它们被指派的子领域。如果用户被指派到多个子领域，他们可以选择查看哪个子领域，一次只能查看一个子领域。在 Enterprise Console 中开启的子领域是活动子领域。用户不能编辑应用于他们的活动子领域之外的策略。

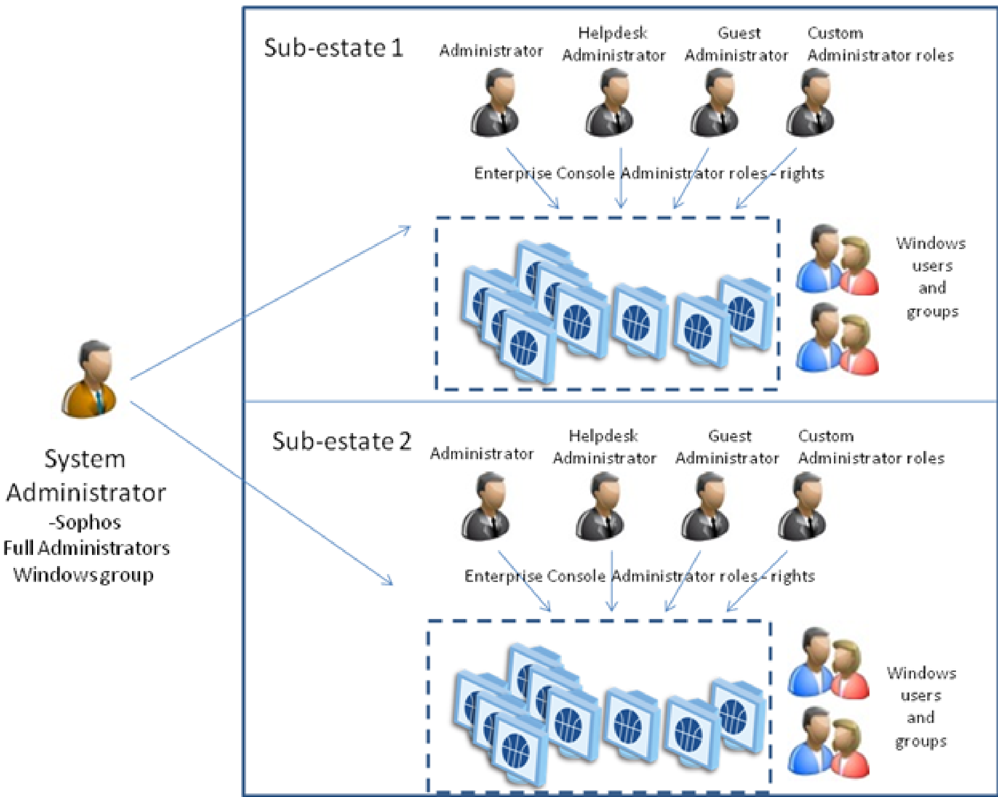


图3：关于角色和子领域

4.2 什么是预设的角色？

在 Enterprise Console 中有四个预设的角色:

角色	描述
系统管理员 (System Administrator)	预置角色，具有管理网络中的 Sophos 安全软件，以及管理 Enterprise Console 中的角色的所有权限。 系统管理员角色不能被编辑或删除。
管理员 (Administrator)	具有权限管理网络中的 Sophos 安全软件，但是不能管理 Enterprise Console 中的角色的预设的角色。 管理员角色可以被重新命名，编辑，或删除。
桌面帮助 (Helpdesk)	只具有调整权限，例如，清除或更新计算机，的预设的角色。 桌面帮助角色可以被重新命名，编辑，或删除。
来宾 (Guest)	只具有读访问 Enterprise Console 权限的预设的角色。 来宾角色可以被重新命名，编辑，或删除。

您可以编辑管理员，桌面帮助，以及来宾角色，或按照 创建角色（第14页）中的说明创建您自己的角色。

4.3 创建角色

如果您已经使用基于角色的管理，您必须具备 **基于角色的管理** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 在 **工具** 菜单中，单击 **管理角色和子领域**。
2. 在 **管理角色和子领域** 对话框的 **管理角色** 标签页中，单击 **创建**。

   会出现 **创建角色** 对话框。

3. 在 **名称** 栏中，输入角色名称。
4. 在 **权限** 窗格板中，选择您想指派给角色的一个或多个角色的权限，并单击 **添加**。
5. 在 **用户和组** 窗格板中，单击 **添加**。
6. 在 **选择用户或组** 对话框，输入想要指派给角色的 Windows 用户或组的名称。单击 **确定**。

   如果需要，按照步骤 5 和 6 中的说明，指定更多的用户或组给角色。

4.4 删除角色

如果您已经使用基于角色的管理，您必须具备 **基于角色的管理** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 在 **工具** 菜单中，单击 **管理角色和子领域**。
2. 在 **管理角色和子领域** 对话框的 **管理角色** 标签页中，选择您想要删除的角色，并单击 **删除**。

   注: 预设的 System Administrator 角色不能被删除。

4.5 编辑角色

如果您已经使用基于角色的管理，您必须具备 **基于角色的管理** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 在 **工具** 菜单中，单击 **管理角色和子领域**。

2. 在 **管理角色和子领域** 对话框的 **管理角色** 标签页中，选择您想要编辑的角色，并单击 **编辑**。

   会出现 **编辑角色** 对话框。

3. 在 **权限** 窗格板中，将权限指派给角色，或者，如需要，删除现有的权限。
4. 在 **用户和组** 窗格板中，添加 Windows 用户或组到角色，或者，如需要，删除现有的用户或组。

4.6 赋予权限给角色

如果您已经使用基于角色的管理，您必须具备 **基于角色的管理** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 在 **工具** 菜单中，单击 **管理角色和子领域**。
2. 在 **管理角色和子领域** 对话框的 **管理角色** 标签页中，选择您想要添加权限的角色，并单击 **编辑**。

   会出现 **编辑角色** 对话框。

3. 在 **权限** 窗格板的 **可用权限** 列表中，选择权限，并单击 **添加**。

4.7 创建子领域

如果您已经使用基于角色的管理，您必须具备 **基于角色的管理** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 在 **工具** 菜单中，单击 **管理角色和子领域**。
2. 在 **管理角色和子领域** 对话框的 **管理子领域** 标签页中，单击 **创建**。

   会出现 **创建子领域** 对话框。

3. 在 **名称** 栏中，输入子领域名称。
4. 在 **Enterprise Console 组** 窗格板中，选择您想要添加子领域的组。
5. 在 **用户和组** 窗格板中，单击 **添加**，以添加 Windows 用户或组到子领域中。

4.8 更改活动子领域

如果您指派了多个子领域，您可以选择当开启 Enterprise Console 时，您想要查看哪个子领域，或者，在 Enterprise Console 中您可以在子领域之间转换。

您一次只能查看一个子领域。 在您更改了活动子领域后，带有新的子领域的 Enterprise Console 会被重载。

要更改活动子领域:

1. 在 **工具** 菜单，单击 **选择活动子领域**。
2. 在 **选择活动子领域** 对话框中，选择您想要打开的子领域，并单击 **确定**。

4.9 编辑子领域

如果您已经使用基于角色的管理，您必须具备 **基于角色的管理** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 在 **工具** 菜单中，单击 **管理角色和子领域**。
2. 在 **管理角色和子领域** 对话框的 **管理子领域** 标签页中，选择您想要编辑的子领域，并单击 **编辑**。
3. 在 **编辑子领域** 对话框中，更改子领域的名称，更改哪些 Enterprise Console 组包括在子领域中，或者，如需要，更改哪些 Windows 用户和组具有访问子领域的权限。 单击 **确定**。

4.10 复制子领域

如果您已经使用基于角色的管理，您必须具备 **基于角色的管理** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 在 **工具** 菜单中，单击 **管理角色和子领域**。
2. 在 **管理角色和子领域** 对话框的 **管理子领域** 标签页中，选择您想要复制的子领域，并单击 **复制**。

   子领域的拷贝会出现在子领域列表中。

3. 选择刚创建的子领域，并单击 **编辑**。 重新命名子领域。 如果您想要，可以更改包括在子领域和/或具有访问该子领域的权限的 Windows 用户和组中的组。

4.11 删除子领域

如果您已经使用基于角色的管理，您必须具备 **基于角色的管理** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 在 **工具** 菜单中，单击 **管理角色和子领域**。
2. 在 **管理角色和子领域** 对话框的 **管理子领域** 标签页中，选择您想要删除的子领域，并单击 **删除**。

   您不能删除**默认的**子领域。

4.12 查看用户或组的角色和子领域

要查看已指派给 Windows 用户或组的角色和子领域:

1. 在 **工具** 菜单中，单击 **管理角色和子领域**。
2. 在 **管理角色和子领域** 对话框的 **用户和组查看** 标签页中，单击 **选择用户或组** 按钮。
3. 在 **选择用户或组** 对话框中，选择您想要查看角色和子领域的用户或组，并单击 **确定**。

4.13 各种权限有权处理什么任务?

权限	任务
计算机搜索，保护和组	开始搜索，停止搜索，为 Network 搜索，IP 范围搜索，以及 Active Directory 搜索查找各个域
	Active Directory 导入计算机和组; import groups from Active Directory 导入组
	从文件中导入计算机
	删除计算机
	保护计算机
	与 Active Directory 同步化组
	更改组的同步化属性
	删除组同步化
	移动计算机
	创建组
	重命名组
	移动组
	删除组
	指派策略到组
自定义数据控制	创建数据控制规则

权限	任务
	编辑数据控制规则
	复制数据控制规则
	删除数据控制规则
	从数据控制扫描中排除文件
	创建内容控制列表
	编辑内容控制列表
	复制内容控制列表
	删除内容控制列表
策略设置 — 防病毒和 HIPS	创建防病毒和 HIPS 策略
	复制防病毒和 HIPS 策略
	重新命名防病毒和 HIPS 策略
	编辑防病毒和 HIPS 策略
	恢复默认的防病毒和 HIPS 设置
	删除防病毒和 HIPS 策略
	从安全隐患控制列表中添加或删除条目
策略设置 — 应用程序控制	创建应用程序控制策略
	复制应用程序控制策略
	重新命名应用程序控制策略
	编辑应用程序控制策略
	恢复默认的应用程序控制设置
	删除应用程序控制策略
策略设置 — 数据控制	创建数据控制策略
	复制数据控制策略
	重新命名数据控制策略
	编辑数据控制策略

权限	任务
	恢复默认的数据控制设置
	删除数据控制策略
策略设置 — 设备控制	创建设备控制策略
	复制设备控制策略
	重新命名设备控制策略
	编辑设备控制策略
	恢复默认的设备控制设置
	删除设备控制策略
策略设置 — 防火墙	创建防火墙策略
	复制防火墙策略
	重新命名防火墙策略
	编辑防火墙策略
	恢复默认的防火墙设置
	删除防火墙策略
策略设置 — NAC	查看 NAC 策略
策略设置 - 介入防范	创建介入防范策略
	复制介入防范策略
	重命名介入防范策略
	编辑介入防范策略
	恢复默认的介入防范设置
	删除介入防范策略
策略设置 — 更新	创建更新策略
	复制更新策略
	重新命名更新策略
	编辑更新策略

权限	任务
	恢复默认的更新设置
	删除更新策略
	创建软件预订
	编辑软件预订
	重新命名软件预订
	复制软件预订
	删除软件预订
	配置更新管理器
调整 — 清除	清除已检测到的项目
	确认已知警报
	确认已知错误
调整 — 更新和扫描	现在更新计算机
	运行完整扫描计算机
	使计算机遵照组策略
报告配置	创建，编辑，或删除报告。
基于角色的管理	创建角色
	重新命名角色
	删除角色
	修改角色的权限
	添加用户或组到角色
	从角色中删除用户或组
	子领域管理：创建子领域；重新命名子领域；删除子领域；添加子领域根组；删除子领域根组；添加用户或组到子领域；从子领域中删除用户或组
系统配置	修改 SMTP 服务器设置；测试 SMTP 服务器设置；修改电子邮件警报收件人

权限	任务
	配置指标面板限制级别
	配置报告发送：配置数据库警报清空；设置在报告中出现的公司名称
	配置发送报告至 Sophos：启用或禁用发送报告至 Sophos；修改用户名；修改电子邮件联系地址
	配置 NAC URL

5 创建和使用组

5.1 组是干什么的？

在保护和管理计算机之前，您必须创建组，并将计算机放到组中。

组是很有用的，因为您可以：

- 从不同的更新源，或者，按照不同的时间计划，更新不同组中的计算机。
- 针对不同的组，使用不同的防病毒和 HIPS 策略，应用程序控制策略，防火墙策略，以及其它策略。
- 更轻松地管理计算机。

提示：您可以在组中创建组，并应用特定的策略集到每个组和子组。

5.2 创建组

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

要创建新的计算机组：

1. 在 **终结点** 视图的 **组** 窗格板（控制台左手边）中，选择您要创建新组的位置。

   如果您要创建一个新的最高一级的组，请单击最高一级的那台计算机的名称。 如果您要创建一个子组，请单击某个现存的组。

2. 在工具栏，单击 **创建组** 图标。

   一个“新组”已被添加到列表中，该组的名称会高亮显示。

3. 为该组输入名称。

更新，防病毒和 HIPS，应用程序控制，防火墙，NAC（网络访问控制），数据控制，以及设备控制策略将会自动应用到新组中。您可以编辑这些策略，或者，应用不同的策略。请参见 编辑策略（第28页）或 指派策略到组（第27页）。

注: 如果新建的组是一个子组，它在创建时会使用它所在的组的设置。

5.3 添加计算机到组

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 选择您要添加到组中的计算机。比如，单击 **未指派** 组，并从中选择计算机。
2. 将所选的计算机拖放到新建的组中。

   如果您从 **未指派** 组中将未受到保护的计算机，移至某一设置了自动更新的组中时，向导程序会启动，指导您为其设置保护。

   如果您将计算机从一个组移到另一个组，它们将采用与所移入的组中的其它计算机相同的策略。

5.4 从组中删除计算机

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以从组中删除计算机，例如，您可以删除已不再在网络中的计算机的条目。

重要: 如果您所删除的是仍然在网络中的计算机，控制台将不会再列示和管理它们。

要删除计算机:

1. 选择您要删除的计算机。
2. 右击并选择 **删除**。

如果您想再次查看该计算机，请单击工具栏中的 **查找新计算机** 图标。这些计算机只有在重新启动后，才会被显示为是已管理的计算机。

5.5 剪切和粘贴组

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 选择您要剪切和粘贴的组。 在 **编辑** 菜单中，单击 **剪切**。
2. 选择您要将剪切下来的组，粘贴到其中的组。 在 **编辑** 菜单中，单击 **粘贴**。

5.6 删除组

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

任何在被删除的组中的计算机，都将被置入 **未指派** 组。

1. 选择您要删除的组。
2. 右击并选择 **删除**。 在得到提示时，确认您想要删除的组，以及它的子组，如果该组带有任何子组。

5.7 重命名组

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 选择您要重新命名的组。
2. 右击并选择 **重新命名**。

5.8 指派策略到组

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 在 **策略** 窗格板中，高亮选择将要应用的策略。
2. 单击该策略，并将其拖放到您想要应用该策略的组中。 在出现提示时，确认您想要继续。

注: 或者，您可以右击某个组，然后，选择 **查看/编辑组策略详情**。 接着，您就可以从下拉菜单中为组选择所要应用的策略。

5.9 查看组采用的策略

要查看哪些策略已被指派到了组中:

- 在 **组** 窗格板中，右击该组。 选择 **查看/编辑组策略详情**。

  在组详情对话框中，您可以查看当前所应用的策略。

6 创建和使用策略

6.1 策略是干什么的?

策略是应用到组中的所有计算机的设置的集合。

- **更新** 策略指定计算机怎样更新安全软件。

  注: 如果您已从 Enterprise Console 3.x 升级，并且尚未迁移您的更新设置，您会看到 **继承性更新** 策略出现在 **更新** 策略旁。要了解更多信息，请参见“继承性更新”部分。

- **防病毒和HIPS策略** 指定安全软件怎样扫描计算机中的病毒，特洛伊木马，蠕虫，间谍软件，广告软件，可能不想安装的应用程序，可疑行为和可疑文件；以及怎样清除它们。
- **应用程序控制** 策略指定在您的计算机上阻断哪些应用程序，允许哪些应用程序。
- **防火墙** 策略指定防火墙怎样保护计算机。
- **数据控制** 策略指定根据文件内容，文件名，或文件类型来监控或限制文件传输的规则。
- **设备控制** 策略指定哪些存储和网络设备不能允许用于工作站计算机上。
- **NAC** 策略指定计算机在能够访问网络之前，必须遵照的各种条件。
- **介入防范** 策略会指定密码，允许经过授权的终结点计算机用户重新配置，禁用，或者，卸载 Sophos 安全软件。

您可以为各种类型创建多个条件。

您可以应用同一策略到多个组。

6.2 什么是默认的策略?

当您安装 Enterprise Console 时，会为您创建默认的策略。

更新策略

默认的更新策略提供:

- 每隔 5 分钟自动从默认的路径更新计算机。默认的路径是一个 UNC 共享路径:\\<计算机名>\SophosUpdate，这里的“计算机名”是更新管理器安装所在的计算机。

注: 如果您已从 Enterprise Console 3.x 升级，并且尚未迁移您的更新设置，您会看到 **继承性更新** 策略出现在 **更新** 策略旁。要了解更多信息，请参见“继承性更新”部分。

防病毒和 HIPS 策略

默认的防病毒和 HIPS 策略提供:

- 读写扫描病毒／间谍软件（但不包括可疑文件，广告软件和其它可能不想安装的应用程序）。
- 分析运行在系统中的程序的执行情况（Sophos Anti-Virus 和 Sophos Endpoint Security and Control for Windows 2000 及以后）。
- 在所涉及的计算机桌面上，显示安全警报，并添加安全警报到事件日志中。

应用程序控制策略

依照默认值，所有的应用程序和应用程序类型都会被允许。读写扫描受控程序是禁用的。

防火墙策略

依照默认值，Sophos Client Firewall 会被启用，并会阻断所有可有可无的网络通讯流。在网络中使用防火墙策略之前，您应该配置它允许您想要使用的应用程序。请参见 设置防火墙（第110页）。

要了解默认的防火墙设置的完整列表，请参见 Sophos 技术支持知识库文章 57757 (*http://cn.sophos.com/support/knowledgebase/article/57757.html*)。

数据控制策略

依照默认值，数据控制是关闭的，并且没有指定任何规则监控或限制因特网中的，或向存储设备进行的文件传输。

设备控制策略

依照默认值，设备控制是关闭的，所有的设备都会被允许。

NAC 策略

依照默认值，计算机可以访问网络（除非您已在 NAC 服务器中修改了默认策略或者更改了“策略模式”）。

介入防范策略

依照默认值，介入防范是关闭的，并且没有指定密码，该密码是允许经过授权的终结点用户重新配置，禁用或卸载 Sophos 安全软件时所需要的。

6.3 需要创建自己的策略吗？

当您安装 Enterprise Console 时，会为您创建“默认的”策略。这些策略会应用到您创建的任何组。

默认的策略提供的是基本的安全保护，但是，如果要使用诸如“网络访问控制”或“应用程序控制”等功能，您需要创建新的策略或更改默认策略。

注: 当您更改默认策略时，更改将应用到您创建的所有策略中。

注: 如果您使用基于角色的管理，那么，您必须具有相应的 **策略设置** 权限，才能创建或编辑策略。例如，您必须具备 **策略设置 - 防病毒和 HIPS** 的权限，才能创建或编辑防病毒和 HIPS 策略。要了解更多信息，请参见 关于角色和子领域（第11页）。

更新策略

默认的更新策略每隔 5 分钟会从默认的路径更新一次计算机。默认的路径是一个 UNC 共享路径：\\<计算机名>\SophosUpdate，这里的“计算机名”是更新管理器安装所在的计算机。您可以指定不同的共享来容纳您所需的软件预定。请参见“配置更新策略”部分。

防病毒和 HIPS

默认的防病毒和 HIPS 策略将保护计算机防范病毒和其它恶意软件。不过，要启用检测其它不想要的应用程序或行为，您可能需要创建新的策略，或者，更改默认策略。请参见 *关于防病毒和 HIPS 策略*（第77页）。

应用程序控制

要定义和阻断未经批准的应用程序，请按照 关于应用程序控制（第120页） 中的说明配置应用程序控制策略。

防火墙策略

要允许真实可信的应用程序访问网络，请按照 设置防火墙（第110页） 中的说明配置防火墙策略。

数据控制

依照默认值，数据控制是关闭的。要防止数据泄露，请按照 关于数据控制（第123页） 中的说明配置数据控制策略。

设备控制

依照默认值，设备控制是关闭的。要限制所允许的硬件设备，请按照 关于设备控制（第138页） 中的说明配置设备控制策略。

NAC

依照默认值，网络访问控制是关闭的。要根据一定的条件限制计算机访问，请按照 *编辑 NAC 策略*（第148页） 中的说明配置 NAC 策略。

介入防范

依照默认值，介入防范是关闭的。要启用介入防范，请按照 关于介入防范（第148页） 中的说明配置介入防范。

6.4 创建策略

如果您使用基于角色的管理，您必须具有相应的 **策略设置** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

要创建策略:

注: 您无法创建 NAC 策略。 您只能编辑它们。 请参见 *编辑 NAC 策略*（第148页）。

1. 在 **终结点** 视图的 **策略** 窗格板中，右击您想要创建的策略的类型，如： “更新策略”， 然后，选择 **创建策略**。

   “新策略”将被添加到列表中，该组的名称会高亮显示。

2. 为该策略输入新的名称。
3. 双击该新策略。 输入您想要的设置。

   要了解怎样选择设置的有关操作指导，请参见配置相关策略的部分。

至此，您已经创建了可以应用到组的策略。

6.5 指派策略到组

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 在 **策略** 窗格板中，高亮选择将要应用的策略。
2. 单击该策略，并将其拖放到您想要应用该策略的组中。在出现提示时，确认您想要继续。

注: 或者，您可以右击某个组，然后，选择 **查看/编辑组策略详情**。接着，您就可以从下拉菜单中为组选择所要应用的策略。

6.6 编辑策略

如果您使用基于角色的管理，那么，:

- 您必须具备相应的 **策略设置** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域 (第11页)。

要编辑一个或多个计算机组的策略:

1. 在 **策略** 窗格板中，双击您想要编辑的策略。
2. 编辑设置。

要了解怎样配置不同策略的操作指导，请参见相关的部分。

6.7 重命名策略

如果您使用基于角色的管理，那么，:

- 您必须具备相应的 **策略设置** 权限，才能执行此任务。
- 您不能重命名应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域 (第11页)。

注: 您不能够重新命名“默认的”策略。

要重命名策略:

1. 在 **策略** 窗格板中，选择您想要重新命名的策略。
2. 右击并选择 **重命名策略**。

6.8 删除策略

如果您使用基于角色的管理，那么，:

- 您必须具备相应的 **策略设置** 权限，才能执行此任务。

- 您不能删除应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

注: 您不能够删除“默认的”策略。

要删除策略:

1. 在 **策略** 窗格板中，右击您想要删除的策略，然后选择 **删除策略**。
2. 任何被删除策略的组，都会恢复使用默认策略。

6.9 查看采用策略的组

要查看某个特定的策略被哪些组采用了:

- 在 **策略** 窗格板中，右击您想要查看的策略，然后选择 **查看使用策略的组**。

  会出现采用了该策略的组的列表。

6.10 检查计算机是否使用组策略

您可以检查是否某个组中的所有计算机都遵照该组的策略。

1. 选择您要检查的组。
2. 在计算机列表的 **终结点** 视图中的 **状态** 标签页中，查看 **策略遵照** 栏。
   - 如果您看到“策略相同”的字样，说明该计算机遵照它所在的组的策略。
   - 如果您看到黄色的警告标志和“策略不同”的字样，说明该计算机使用的策略与它所在的组中的其它计算机使用的策略不同。

   要了解更多有关计算机的安全功能的状态，以及应用到计算机上的策略的详细信息，请参见 **终结点** 视图中相应的标签页，例如，**防病毒详情** 标签页。

如果您想要计算机遵照它们所在的组的策略，请参见使计算机采用组策略（第29页）。

6.11 使计算机采用组策略

如果您使用基于角色的管理，您必须具备 **调整-更新和扫描** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

如果您发现计算机没有遵照它所在的组的策略，您可以将组策略应用到该计算机上。

1. 选择没有遵照组策略的一个或数个计算机。

2. 右击并选择 **遵照**。 然后选择相应的策略类型，例如：**组防病毒和 HIPS 策略**。

7 查找网络中的计算机

7.1 选择怎样查找计算机

您可以通过“查找新计算机”功能，在使您能够查找网络计算机的几个选项中选择查找计算机的方法，并将它们添加到 Enterprise Console 中。 有以下几个选项：

- 从 *Active Directory* 中导入容器和计算机（第30页）
- 通过 *Active Directory* 查找计算机（第31页）
- 通过浏览网络查找计算机（第31页）
- 通过 *IP* 地址范围查找计算机（第32页）
- 从文件中导入计算机（第33页）

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能添加计算机到控制台中。 要了解更多信息，请参见 关于角色和子领域（第11页）。

7.2 从 Active Directory 中导入容器和计算机

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

从 Active Directory 中导入组可以获取 Active Directory 容器结构，将该它复制到 Enterprise Console 中作为计算机组的结构。您可以只导入组结构，或同时导入组和计算机。如果您选择后者，在 Active Directory 中找到的计算机会被放置到他们各自的组中，而不是放置到 **未指派** 组中。

您可以同时拥有自己创建和管理的“普通”的组，以及从 Active Directory 导入的组。您还可以将导入的组与 Active Directory 同步化。

要从 Active Directory 中导入组：

1. 在工具栏中，单击 **查找新计算机** 图标。

2. 在 **查找新计算机** 对话框的 **从 Active Directory 导入** 窗格板中，选择 **导入** 并单击 **确定**。

   或者，选择一个您想将 Active Directory 容器导入的组，右击并选择 **从 Active Directory 导入**。

   从 Active Directory 导入向导 会启动。

3. 请按照向导中的操作指导做。在被询问选择导入什么时，根据您想要导入什么，选择 **计算机和组** 或 **仅限于组**。

在您从 Active Directory 中导入容器之后，请应用策略到组中。请参见“创建和使用策略”部分。

在您将组策略应用到组之后，如果您愿意，您可以将这些组与 Active Directory 同步化。要了解操作指导，请参见 *与 Active Directory 同步化*（第36页）。

7.3 通过 Active Directory 查找计算机

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以使用 Active Directory 查找网络中的计算机，并将它们添加到 **未指派** 组中。

1. 在工具栏中，单击 **查找新计算机** 图标。
2. 在 **查找新计算机** 对话框中，选择 **通过 Active Directory 查找** 并单击 **确定**。
3. 您会被提示输入用户名和密码。 如果您需要提供帐户详情，才能访问的计算机（如： Windows XP SP 2），您就需要输入用户名和密码。

   该帐户必须是域管理员帐户，或者，对所要操作的 Windows XP 计算机有完全的管理权限。

   如果您使用域帐户名，您必须以“域名\用户”的形式输入用户名。
4. 在 **查找计算机** 对话框中，选择您想搜索的域。 单击 **确定**。
5. 单击 **未指派** 组，可以查看已经找到的计算机。

开始管理这些计算机之前，请选择它们，并将它们拖放到组中。

7.4 通过浏览网络查找计算机

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

要将在 Windows 域和工作组中找到的计算机的列表添加到 **未指派** 组中。

1. 在工具栏中，单击 **查找新计算机** 图标。
2. 在 **查找新计算机** 对话框中，选择 **在网络中查找** 并单击 **确定**。
3. 在 **认证资料** 对话框中，输入具备足够权限获得计算机信息的帐户的用户名和密码。

   该帐户必须是域管理员帐户，或者，对所要操作的计算机有完全的管理权限。 如果您使用域帐户名，您必须以“域名\用户”的形式输入用户名。

   如果您所要操作的计算机无需帐户详情即可访问，那么，您可以跳过此步骤。
4. 在 **查找计算机** 对话框中，选择您想搜索的域或工作组。 单击 **确定**。
5. 单击 **未指派** 组，可以查看已经找到的计算机。

开始管理这些计算机之前，请选择它们，并将它们拖放到组中。

7.5 通过 IP 地址范围查找计算机

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以使用 IP 地址范围查找网络中的计算机，并将它们添加到 **未指派** 组中。

注: 您无法使用 IPV6 地址。

1. 在工具栏中，单击 **查找新计算机** 图标。
2. 在 **查找新计算机** 对话框中，选择 **通过 IP 地址范围查找** 并单击 **确定**。
3. 在 **认证资料** 对话框中，您会被提示输入用户名和密码。 如果您需要提供帐户详情，才能访问的计算机（如：Windows XP SP 2），您就需要输入用户名和密码。

   该帐户必须是域管理员帐户，或者，对所要操作的 Windows XP 计算机有完全的管理权限。

   如果您使用域帐户名，您必须以“域名\用户”的形式输入用户名。

   在 **SNMP** 窗格板中，您可以输入 SNMP 团体名。
4. 在 **查找计算机** 对话框中，输入 **IP 地址范围起点** 和 **IP 地址范围终点**。 单击 **确定**。
5. 单击 **未指派** 组，可以查看已经找到的计算机。

开始管理这些计算机之前，请选择它们，并将它们拖放到组中。

7.6 从文件中导入计算机

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域 (第11页)。

要使 Enterprise Console 列示您的计算机，您可以从文件中导入计算机名称。

包含计算机名称的文件，必须是下列之一:

- 符合下列要求的文件
- 从 Sophos SAVAdmin 中导出的 SGR 文件

您可以按以下形式创建文件：

```
[GroupName1] Domain1|Windows2000|ComputerName1
Domain1|Windows2000Server|ComputerName2
```

注: 您不一定非要指定计算机防置在哪个组中，如果您输入 [] （括号之间没有空格）作为组名，计算机将被放置在 **未指派** 组中。

注: 有效的操作系统名称如下： Windows95，Windows98，Windows9x，WindowsMe，WindowsNT，WindowsNTServer，Windows2000，Windows2000Server，WindowsXP，Windows2003，WindowsVista，Windows7，WindowsServer2008，WindowsServer2008R2，MACOS9，MACOSX，Linux，以及 Unix。

域名和操作系统都是可选项。所以，也可能有以下形式:

```
[GroupName1] ComputerName1
```

您可以按以下说明，导入计算机名:

1. 在 **文件** 菜单中，单击 **从文件中导入计算机**。
2. 在打开的窗口中，选择导入计算机名称的文件。
3. 单击 **未指派** 组，可以查看已经找到的计算机。
4. 开始管理这些计算机之前，请选择它们，并将它们拖放到组中。

8 与 Active Directory 同步化

8.1 关于与 Active Directory 同步化

本节概述 Active Directory 同步化。

Active Directory 同步化能做什么？

与 Active Directory 同步化，您可以将 Enterprise Console 组与 Active Directory 容器同步化。 在 Active Directory 中找到的新计算机和容器会被自动复制到 Enterprise Console 中。 您还可以选择自动保护找到的 Windows 2000 或以后的工作站。这将最大限度地缩短计算机可能感染到病毒的时间，同时减少您安排保护计算机所需要做的大量工作。

注: 运行 Windows 95/98，Windows Server，Mac，Linux，或 UNIX 等操作系统的计算机不会自动受到保护。 您必须手动保护这样的计算机。

在设置了同步化之后，您可以设置在今后的同步化中，向指定的收件人发送有关找到新的计算机和容器的电子邮件警报。 如果您选择了自动保护已同步化的 Enterprise Console 组中的计算机，那么，您还可以设置在自动保护失败时，发出警报。

Active Directory 同步化怎样工作？

在 Enterprise Console 中，您可以同时具有您自己管理的“普通的”，未同步化的组，以及与 Active Directory 同步化的组。

在设置同步化时，您选择或创建一个同步化点，一个将要与某个 Active Directory 容器同步化的 Enterprise Console 组。 Active Directory 容器中所有子组和计算机都将被复制到 Enterprise Console 中，并被保持与 Active Directory 同步化。

注: 要了解更多有关同步化点的信息，请参见 什么是同步化点? （第35页）。要了解更多有关同步化组的信心，请参见什么是已同步化的组? （第35页）。

在您设置了与 Active Directory 同步化之后，Enterprise Console 中的已同步化的组的结构，与其在 Active Directory 容器中与之同步化的组的结构是完全一致的。 这意味着:

- 如果新的计算机添加到 Active Directory 容器中，那么，它同样会出现在 Enterprise Console 中。
- 如果某计算机从 Active Directory 中删除，或者被已移动到未同步化的容器中，那么，在 Enterprise Console 中该计算机会被移动到**未指派**组中。

  注: 当某个计算机被移至**未指派**组中后，它将停止接收新的策略。

- 如果某计算机从一个同步化的容器中移到另一个同步化的容器中，那么，该计算机从一个 Enterprise Console 组中移到另一个 Enterprise Console 组。
- 如果某计算机在首次同步化时，已经在某个 Enterprise Console 组中，那么，它会被从该组中移动到与 Active Directory 相对应的那个 Enterprise Console 同步化的组中。

■ 当某个计算机被移至策略不同的新组中时，新的策略会被发送给该计算机。

依照默认值，同步化会每 60 分钟进行一次。 如果您愿意，您可以更改该同步化进行的频率。

怎样运用同步化?

使哪些组与 Active Directory 同步化，以及设置多少同步化点，将完全由您来决定。 您必须考虑，将要创建的组在同步化之后的大小，是能够易于管理的。您应该能够方便地部署软件，扫描和清除计算机。这对于进行首次部署尤其重要。

建议的做法如下:

1. 使用 **从 Active Directory 导入** 功能，导入组结构（没有计算机）。 要了解操作指导，请参见 *从 Active Directory 中导入容器和计算机*（第30页）。
2. 查看导入的组结构，并选择同步化点。
3. 设置组策略，并应用它们到组和子组。 要了解操作指导，请参见 创建策略（第27页） 和 指派策略到组（第27页）。
4. 与 Active Directory 同步化您选择的同步化点，一次进行一个同步化点。 要了解操作指导，请参见 *与 Active Directory 同步化*（第36页）。

8.2 什么是同步化点?

同步化点是一个指向 Active Directory 中的某个容器（或子树）的一个 Enterprise Console 组。同步化点可以容纳从 Active Directory 中导入的已同步化的组。

在 **组** 窗格板中，同步化点会显示如下:



您可以移动，重命名，或删除同步化点。您还可以更改策略和同步化策略，包括对同步化点的自动保护设置。

您不能在同步化点中创建或删除子组，或将其它组移动到同步化点中。您不能将计算机移至或移出同步化点。

8.3 什么是已同步化的组?

已同步化的组 是从 Active Directory 中导入的同步化点中的子组。

在 **组** 窗格板中，已同步化的组会显示如下:



您可以更改指派到已同步化的组中的策略。

您不能更改除了组策略以外的任何已同步化的组的设置。您不能重命名，移动，或删除已同步化的组。您不能将计算机或组移至或移出已同步化的组中。您不能在已同步化的组中创建或删除子组。您不能更改已同步化的组的同步化设置。

8.4 与 Active Directory 同步化

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

要与 Active Directory 同步化:

1. 选择将要作为同步化点的计算机组，单击鼠标右键，并选择 **与 Active Directory 同步化**。

   与 Active Directory 同步化 向导会启动。

2. 在向导的 **概述** 页面中，单击 **下一步**。
3. 在 **选择一个 Enterprise Console 组** 页面中，选择或创建一个，您想保持与 Active Directory 同步化（同步化点）的 Enterprise Console 组。单击 **下一步**。
4. 在 **请选择一个 Active Directory 容器** 对话框中，选择一个组将用来与之同步化的 Active Directory 容器。请输入容器的名称，（例如，LDAP://CN=Computers,DC=domain_name,DC=local），或者，单击 **浏览** 找到 Active Directory 中的该容器。单击 **下一步**。

   重要: 如果某个计算机存在于多个已同步化的 Active Directory 容器中，那么，它会出问题，会不断地在计算机和 Enterprise Console 之间交换消息。各个计算机应该只在 Enterprise Console 中列示一次。

5. 如果您想要自动保护 Windows 2000 或以后的工作站计算机，请在 **自动保护计算机** 页面，勾选 **自动安装 Sophos 安全软件** 勾选框，然后，选择您想要安装的软件。

   如果您想自动删除其它软件商的类似软件，请保留选择 **第三方安全软件检测**。

   如果您需要删除其它软件公司的更新工具，请参见删除第三方安全软件（第42页）。

   注:

   您无法在运行服务器操作系统，或者运行 Windows Vista Starter 的计算机上安装防火墙。

   您必须单击链接，指定 NAC 服务器的 URL 之后，才能将 Sophos NAC 安装到计算机上。

   从现在起，所有在同步化过程中找到的 Windows 2000 或以后的工作站，都将自动被保护，并遵照它们各自的组策略。

   重要: 运行 Windows 95/98，Windows server，Mac OS，或 Linux 等操作系统的计算机，不会自动被保护。您必须按照 *Sophos Endpoint Security and Control* 高级安装指南 中的说明，手动保护此类计算机。

   注: 您稍后可以在 **同步化属性** 对话框中，启用或禁用自动保护。要了解操作指导，请参见 查看和编辑同步化属性（第39页）。

   单击 **下一步**。

6. 如果您选择自动保护计算机，请在 **请输入 Active Directory 认证资料** 页面中，输入将要用来在计算机上安装软件的系统管理员帐户的详情。单击 **下一步**。

7. 在 **请选择同步化频率** 页面中，选择您想要 Enterprise Console 组与 Active Directory 容器同步化的频率。默认值是 60 分钟。

   注: 您稍后可以在 **同步化属性** 对话框中，更改同步化频率。要了解操作指导，请参见 查看和编辑同步化属性（第39页）。

8. 在 **确认您的选择** 页面中，检查详情，然后单击 **下一步** 继续。

9. 在向导的最后一页中，您可以查看已同步化的组，计算机的详情。

   您还可以设置电子邮件警报，以便在今后的同步化过程中，找到新的计算机和组时，可以向您所选择的收件人寄送警报。如果您选择了自动保护已同步化的组中的计算机，那么，您还可以设置在自动保护失败时，发出警报。要在您单击 **完成** 之后，打开 **配置电子邮件警报** 对话框，请勾选向导最后一页中的勾选框。要了解操作指导，请参见 设置 *Active Directory* 同步化电子邮件警报（第158页）。

   要关闭向导，请单击 **完成**。

8.5 使用同步化自动保护计算机

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

在与 Active Directory 同步化的过程中找到的计算机中，运行 Windows 2000 或以后的计算机会获得自动保护。

重要: 运行 Windows 95/98，Windows Server，Mac OS，Linux，或 Unix 等操作系统的计算机，不会自动被保护。您必须按照 *Sophos Endpoint Security and Control 高级安装指南* 中的说明，手动保护此类计算机。

您可以在设置同步化时（请参见 与 *Active Directory* 同步化（第36页）），或在稍后编辑同步化属性时，自动保护已同步化的组中的计算机。

以下的操作指导，说明怎样通过编辑同步化属性，来保护计算机。

1. 在 **组** 窗格板中，选择您想要为之启用自动保护的组（同步化点）。右击该组，然后选择 **同步化属性**。
2. 在 **同步化属性** 对话框中，勾选 **自动安装 Sophos 安全软件** 勾选框，然后，选择您想要安装的软件。

   如果您想自动删除其它软件商的类似软件，请保留选择 **第三方安全软件检测**。

   如果您需要删除其它软件公司的更新工具，请参见 删除第三方安全软件（第42页）。

   注:

   您无法在运行服务器操作系统，或者运行 Windows Vista Starter 的计算机上安装防火墙。

   您必须单击链接，指定 NAC 服务器的 URL 之后，才能将 Sophos NAC 安装到计算机上。

3. 输入将要用来在计算机上安装软件的系统管理员帐户的详情。单击 **确定**。

如果您将来想要禁用自动保护，请在 **同步化属性** 对话框中，取消勾选 **自动安装 Sophos 安全软件** 勾选框。

8.6 查看和编辑同步化属性

如果您使用基于角色的管理，那么，您必须具备**计算机搜索，保护和组**权限，才能编辑组同步化属性。要了解更多信息，请参见 关于角色和子领域（第11页）。

要查看和编辑同步化属性:

1. 在 **组** 窗格板中，选择您想要为之编辑同步化属性的组（同步化点）。右击该组，然后选择 **同步化属性**。

   会出现 **同步化属性** 对话框。

2. 在 **Active Directory 容器** 栏，您可以看到组与之同步化的容器。如果您想要将组与不同的容器同步化，请删除同步化，然后，再次运行 **与 Active Directory 同步化** 向导。请参见 开启或关闭同步化（第40页） 和 与 *Active Directory* 同步化（第36页）。
3. 在 **同步化频率** 栏中，设定同步化频率。默认值是 60 分钟。最小值是 5 分钟。
4. 如果您想要自动保护所有找到的新的 Windows 2000 或以后的工作站，并遵照它们各自的组策略，请选择 **自动安装 Sophos 安全软件**。在 **功能** 下，已默认选择防病毒保护。如果想安装其它的 Sophos 安全软件，请勾选相应的勾选框。输入将要用来在计算机上安装软件的系统管理员帐户的详情。

   注:

   您无法在运行服务器操作系统，或者运行 Windows Vista Starter 的计算机上安装防火墙。

   您必须单击链接，指定 NAC 服务器的 URL 之后，才能将 Sophos NAC 安装到计算机上。

注: 只有 Windows 2000 或以后的工作站才能获得自动保护。运行 Windows 95/98，Windows Server，Mac OS，Linux，或 UNIX 等操作系统的计算机，不能自动被保护。您必须按照 *Sophos Endpoint Security and Control* 高级安装指南 中的说明，手动保护此类计算机。

8.7 立即与 Active Directory 同步化

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以立即与 Active Directory 容器同步化 Enterprise Console 组（同步化点），不用等到计划中的下一次同步化。

要立即与 Active Directory 同步化:

1. 在 **组** 窗格板中，选择您想要与 Active Directory 同步化的组（同步化点）。右击该组，然后选择 **同步化属性**。
2. 在 **同步化属性** 对话框中，进行相应的更改，然后，单击 **确定**。

8.8 开启或关闭同步化

如果您使用基于角色的管理，您必须具备 **计算机搜索，保护和组** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

- 要开启同步化，请按照 *与 Active Directory 同步化*（第36页） 中的说明，运行 **与 Active Directory 同步化** 向导。
- 要关闭同步化，请选择您不再想要其与 Active Directory 同步化的组（**同步化点**），右击该组，并选择 删除同步化。 单击 **是** 确认。

9 保护计算机

9.1 准备安装防病毒软件

在确保计算机满足总的系统要求的同时，在能够自动安装软件之前，您必须完成几个步骤。

要准备安装防病毒软件:

1. 在 Windows Vista 计算机上:

   a) 确保 Remote Registry Service 已启动，并且它的启动类型设置为 自动。 启动此服务并不是 Windows Vista 的默认设置。

   b) 关闭 用户帐户控制。 当安装完成时，您应该重新开启用户帐户控制。

   c) 关闭 共享向导。

   d) 使用“控制面板”中的 **管理工具**，打开 高级安全 Windows 防火墙。 确保允许 **流入连接**。

   e) 更改 **入站规则** 启动以下进程。 在安装完成后，重新禁用它们。

   Remote Administration (NP-In) 域

   Remote Administration (NP-In) 专有

   Remote Administration (RPC) 域

   Remote Administration (RPC) 专有

   Remote Administration (RPC-EPMAP) 域

   Remote Administration (RPC-EPMAP) 专有

2. 在 Windows 2003/XP Pro/2000/NT 计算机上:

   a) 确保 Remote Registry，Server，Computer Browser，以及 Task Scheduler 等服务都已启动。

   b) 确保 C$ admin 共享已启用。

   c) 确保已关闭“简单文件共享”（仅限 Windows XP 计算机）。

3. 在 Windows XP SP2 或 SP3 计算机上:

   a) 确保 Remote Registry，Server，Computer Browser，以及 Task Scheduler 等服务都已启动。

   b) 确保 C$ admin 共享已启用。

   c) 确保已关闭“简单文件共享”

   d) 为 Microsoft 网络启用文件和打印机共享。

   e) 确保开启了 TCP 端口 8192，8193，以及 8194。

   f) 重新启动计算机，使改动生效。

9.2 删除第三方安全软件

如果您想要删除任何先前安装的安全软件，那么，在 **保护计算机向导** 中勾选 **检测第三方安全软件** 选项之前，请按照以下说明做:

- 如果计算机上运行的是其它软件商的防病毒软件，请确保该软件的用户界面已关闭。
- 如果计算机上运行的是其它软件商的防火墙软件或 HIPS 软件，请确保该软件已关闭，或已配置为允许运行 Sophos 安装程序。
- 如果您想删除的不仅是其它软件商的软件，而且还包括它的更新工具（以避免它重新自动安装该软件），请按照以下步骤做：如果计算机没有安装更新工具，您可以忽略以下步骤。

注: 您必须从本地重新启动您从中删除了第三方防病毒软件的所有计算机。

如果计算机上安装了其它软件商的更新工具，并且您希望删除该更新工具，那么，在勾选 **保护计算机** 向导中的 **第三方安全软件检测** 之前，您需要修改配置文件:

注: 如果计算机运行了其它软件商的防火墙或 HIPS产品，那么，您可能需要保留该软件商的更新工具。请参见该软件商的技术文档，了解详情。

要修改配置文件:

1. 在中央安装目录中，找到 data.zip 文件。
2. 从 data.zip 文件中提取 crt.cfg 配置文件。
3. 编辑该 crt.cfg 文件，更改行 "RemoveUpdateTools=0" 为 "RemoveUpdateTools=1"。
4. 保存您的更改，并保存 crt.cfg 到 data.zip 文件所在的同一个目录中。不要将 crt.cfg 文件放回 data.zip 中，否则，在下一次更新 data.zip 文件时，它会被覆盖。

当您运行 **保护计算机** 向导，并选择 **第三方安全软件检测**，修改了的配置文件会删除任何第三方安全软件的更新工具，以及第三方安全软件。

9.3 保护计算机

在您从控制台中保护计算机之前:

- 在保护组中的计算机之前，您必须应用某个更新策略到该组。
- 如果您从控制台自动保护 Windows XP 计算机，请确保“简单文件共享”已关闭。

- 如果您使用基于角色的管理，那么，您必须具备 **计算机搜索，保护和组** 权限，才能保护计算机。要了解更多信息，请参见 关于角色和子领域（第11页）。

自动安装不能在 Windows 95/98，Mac，Linux，和 UNIX 计算机上进行。请用手动安装代替。要了解操作指导，请参见 *Sophos Endpoint Security and Control* 高级安装指南。Sophos 技术文档发布在 *http://cn.sophos.com/support/docs/* 中。

如果您选择了与 Active Directory 同步化，并自动保护计算机，那么，您不需要执行以下步骤。要了解详情，请参见 关于与 *Active Directory* 同步化（第33页）以及其它相关的主题。

要保护计算机:

1. 根据您想要保护的计算机是否已在计算机组中，按照以下说明之一做:
   - 如果您想要保护的计算机在 **未指派** 组中，请将该计算机拖放到其它某个组中。
   - 如果您想要保护的计算机已在某个计算机组中，请选择该计算机，单击鼠标右键，然后，单击 **保护计算机**。

   会启动 **保护计算机向导**。

2. 请按照向导中的操作指导做。在 **选择功能** 页中，选择您想要的功能。
   防病毒保护总是会被选择，必须被安装。您还可以选择安装以下功能:
   - **Compliance Control** （一种 Sophos NAC 代理）

     Compliance Control 只有包含在您的用户授权使用许可中时，才会被提供，而且只能用于 Windows 2000 或以后的操作系统中。

     您必须先指定 NAC 服务器的 URL，然后，才能使用 Compliance Control。如果安装 Sophos NAC 的是多台服务器，那么，请使用运行了 Application Server 的那台服务器的 URL，而不要使用安装了数据库的那台服务器的 URL。
   - **Sophos Client Firewall**

     Sophos Client Firewall 只有包含在您的用户授权使用许可中时，才会被提供，而且只能用于 Windows 2000 或以后的操作系统中。

     您无法在运行服务器操作系统，或者运行 Windows Vista Starter 的计算机上安装防火墙。
   - **第三方安全软件检测**

     如果您想自动删除其它软件商的类似软件，请保留选择 **第三方安全软件检测**。第三方软件检测，仅卸载与您所要安装的产品的功能相同的那些产品。

3. 在 **保护摘要** 页中，安装中的任何问题都会显示在 **保护问题** 栏中。安装过程的排疑解难（请参见 *Sophos Endpoint Security and Control* 安装失败（第175页）），或者，在这些计算机上进行手动安装（请参见 *Sophos Endpoint Security and Control* 高级安装指南）。单击 **下一步**。
4. 在 **认证资料** 页中，输入可以用来安装软件的帐户的详情。

   该帐户通常都是域系统管理员帐户。它必须:

   - 拥有您要保护的计算机的管理员权限
   - 可以登录您安装了 Management Server 的那台计算机。
   - 可以读取在 **更新** 策略中，所指定的主服务器的路径。请参见选择更新源（第96页）。

   注: 如果您使用域帐户名，您必须以 域名\用户 的形式输入用户名。

   如果计算机在同一 Active Directory 架构覆盖的不同的域中，那么，请在 Active Directory 中使用 Enterprise Administrator 帐户。

9.4 查看引导路径

如果 Enterprise Console 不能在某些计算机上自动安装防病毒，防火墙，或 NAC 等功能，您可以实行手动安装。

要找到安装程序:

1. 在 **查看** 菜单中，单击 **引导路径**。
2. 在 **引导路径** 对话框中，对于每个软件预订，您将看到包含软件的安装程序的路径，以及支持该软件的操作平台和软件的版本。 记录下您所需要的安装程序的路径。

   如果您的用户授权使用许可协议中包括防火墙，您就可以与防病毒软件，NAC 一道，将其安装到 Windows 2000 或以后的计算机上。 包含了所有功能的那个安装程序，在目录 SAVSCFXP 中。

要了解怎样在不同的操作系统上手动安装安全软件的信息，请参见 *Sophos Endpoint Security and Control* 高级安装指南。

10 检查网络是否受到保护

10.1 怎样检查网络是否受到保护?

要了解网络安全状态的“一览图”，请使用指标面板。要了解更多信息，请参见指标面板概述（第45页） 和 配置指标面板（第47页）。

您可以通过使用计算机列表和计算机列表过滤器，识别有问题的计算机。 例如，您可以查看哪些计算机没有安装防火墙，或者，出现了需要注意的警报。要了解更多信息，请参见 检查计算机是否受到保护（第48页），检查计算机是否及时更新（第49页），和 查找有问题的计算机（第49页）。

您还可以检查是否组中所有的计算机都遵照该组的策略，具体说明请见检查计算机是否使用组策略（第29页）。

10.2 指标面板概述

使用指标面板检查您的网络安全状况。要显示或隐藏指标面板，请单击工具栏上的 **指标面板** 按钮。



图4：指标面板

指标面板界面

指标面板由以下七个部分组成：

计算机

此部分显示网络中的计算机的总数，以及联网的，已管理的，未管理的计算机的数量。

要查看已管理的，未管理的，联网的，或所有计算机的列表，请单击 **计算机** 栏中的链接之一。

更新文件

此部分显示更新管理器的状态。

具有警报的计算机

此部分显示具有下列类型的警报的，已管理的计算机的数量和百分比：

- 已知的和未知的病毒和间谍软件
- 可疑行为和文件

- 广告软件和其它可能不想安装的应用程序

要查看具有未处理的警报的已管理的计算机的列表，请单击栏目标题：**具有警报的计算机**。

超过事件限制级别的计算机

此部分显示在最近 7 天中，超过事件限制级别的计算机的数量。

要查看具有设备控制事件，数据控制事件，受控程序事件，或防火墙事件的计算机列表，请在 **超过事件限制级别的计算机** 部分单击相应的链接。

策略

此部分显示具有组策略不一致，或者策略比较出错的，已管理的计算机的数量和百分比。它还包括控制台已向其发出已更改的策略，但尚未回应的计算机。

要查看具有不一致策略的已管理的计算机的列表，请单击栏目标题：**策略**。

保护

此部分显示 Sophos Endpoint Security and Control 或 Sophos Anti-Virus 未及时更新，或者使用未知的检测数据的，已管理的联网计算机的数量和百分比。

要查看未及时更新的已管理的联网计算机的列表，请单击栏目标题：**保护**。

错误

此部分显示具有未处理的扫描，更新，或防火墙错误的受管理的计算机的数量或百分比。

要查看具有未处理的 Sophos 产品错误的已管理的计算机的列表，请单击栏目标题：**错误**。

指标面板安全状态指示器

指标面板可以显示三种安全状态指示器。

标志	释意
✔	绿色的指示器，表示“普通”状态。受影响的计算机的数量低于警告级指标。
!	黄色的指示器，表示“警告”状态。已达到警告级指标。
⚠	红色的指示器，表示“紧要”状态。已达到紧要级指标。

指示器出现在各个部分，以及出现在整个指标面板中。

注: 指标面板部分的健康指示器 是出现在指标面板部分右上角的栏目标题旁的图标，它显示所在的部分所表示的特定领域的安全状态。

指标面板部分的健康指示器，显示某个部分的最高程度的安全状态，它们是:

- 只要有一个指示器的指标达到了警告级，指标面板部分的健康指示器就会从“普通”变为“警告”。
- 只要有一个指示器的指标达到了紧要级，指标面板部分的健康指示器就会从“警告”变为“紧要”。

注: 网络综合健康指标 是出现在 Enterprise Console 窗口的右下角状态栏中的一个图标，它显示整个网络的综合安全状态。

网络综合健康指示器，显示指标面板部分的最高程度的安全状态，它们是:

- 只要有一个指标面板指示器的指标达到了警告级，网络综合健康指示器就会从“普通”变为“警告”。
- 只要有一个指标面板指示器的指标达到了紧要级，网络综合健康指示器就会从“警告”变为“紧要”。

当您首次安装或更新 Enterprise Console 时，指标面板会使用默认中警告和紧要级设置。您可以在 **配置指标面板** 对话框中，配置自己的警告和紧要级设置。要了解怎样做，请参见 配置指标面板（第47页）。

您还可以设置电子邮件警报，当指标面板中的某部分达到了“警告级”或“紧要级”时，可以向您所选择的收件人寄送警报。要了解怎样做，请参见设置网络状态电子邮件警报（第157页）。

10.3 配置指标面板

如果您使用基于角色的管理，那么，您必须具有 **系统配置** 权限，才能配置指标面板。要了解更多信息，请参见 关于角色和子领域（第11页）。

指标面板显示警告，或者，紧要状态指标。这些指标基于具有未处理的警报或错误的已管理的计算机的百分比；或者，基于最近一次从Sophos更新的时间。

您可以设置您想要使用的“警告级”和“紧要级”设置。

1. 在 **工具** 菜单中，单击 **配置指标面板**。

2. 在 **配置指标面板** 对话框的 **警告级** 和 **紧要级** 文本框中，按照以下说明更改指标级别值。

   a) 在 **具有未处理的警报的计算机**，**具有Sophos产品错误的计算机**，以及 **策略和保护** 下，输入受到特定的问题影响的已管理的计算机的百分比，该值会触发相应的指示器从“警告”转为“紧要”。

   b) 在 **发生事件的计算机** 窗格板中，输入事件数，如果该数量的事件在7日之内发生，就会触发显示在指标面板中的警报。

   c) 在 **来自Sophos的最新保护措施** 下，输入以小时计的，从上一次自 Sophos 成功完成更新的时间间隔，该值会触发“更新”指示器从“警告”转为“紧要”。 单击 **确定**。

   如果您设置级别的值为零，那么，只要出现第一个警报，警告就会被触发。

您还可以设置电子邮件警报，当达到了“警告级”或“紧要级”时，可以向您所选择的收件人寄送警报。 要了解怎样做，请参见 设置网络状态电子邮件警报 （第157页）。

10.4 检查计算机是否受到保护

如果计算机中运行了读写扫描和开启了防火墙（如果安装了），计算机就受到了保护。 要获得完全的保护，软件还必须及时更新。

注: 您也许选择了，在某种特定的计算机上，比如：文件服务器，不使用读写扫描。 在这种情况下，请确保这些计算机使用了计划扫描，并且使用的是最新的防病毒软件版本。

要检查计算机是否受到保护:

1. 选择您要检查的计算机所在的组。
2. 如果您要检查在该组中的子组里的计算机，请在顶部的下拉列表中选择 **在这一级，及以下级**。
3. 在计算机列表中的 **状态** 标签页中，查看 **读写扫描** 栏。

   如果看到“活动”字样，则该计算机上正在运行读写扫描。 如果看到的是灰色的盾牌，则该计算机上没有运行读写扫描。

4. 如果您安装了防火墙，请查看 **防火墙已启用** 栏。

   如果您看到“是”字样，则防火墙是启用的。 如果您看到灰色的防火墙图标和“否”字样，则防火墙是禁用的。

5. 如果您使用其它功能，如：应用程序控制或数据控制，请检查相应的栏中的状态。

要了解有关怎样检查计算机是否及时更新的信息，请参见检查计算机是否及时更新（第49页）。

要了解通过计算机列表筛选查找有问题的计算机的信息，请参见查找有问题的计算机（第49页）。

10.5 检查计算机是否及时更新

如果您是依照建议设置的 Enterprise Console，计算机应该自动收到更新文件。

要检查计算机是否及时更新:

1. 选择您要检查的计算机所在的组。
2. 如果您要检查在任何子组里的计算机，请在顶部的下拉列表中选择 **在这一级，及以下级**。
3. 在 **状态** 标签页中，查看 **及时更新** 栏，或者，转到 **更新详情** 标签页。
   - 如果您在 **及时更新** 栏中看到“是”字样，那么，该计算机已及时更新。
   - 如果看到一个钟的图标，则该计算机使用的是未及时更新的防病毒软件版本。旁边的文字，说明是该计算机已有多长时间没有及时更新了。

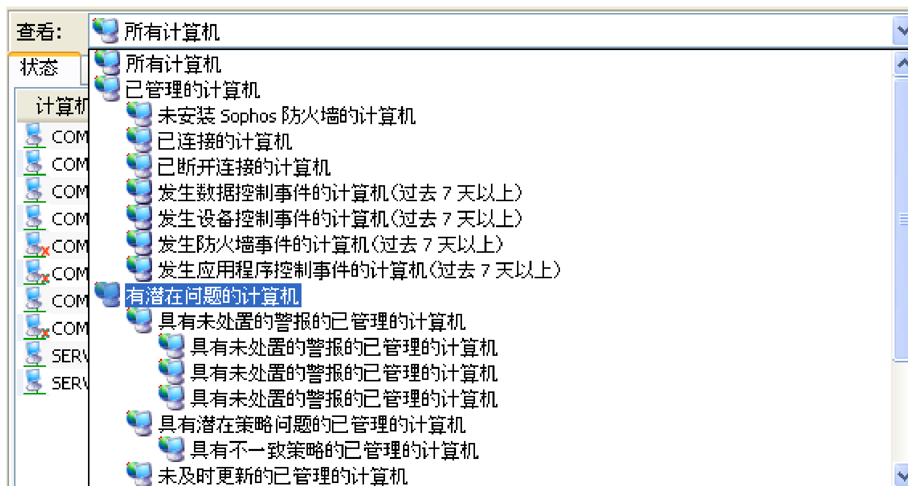
要了解更多有关更新诸如未及时更新的计算机的信息，请参见更新未及时更新的计算机（第63页）。

10.6 查找有问题的计算机

要显示没有妥善保护的，或者，存在其它保护方面的问题的计算机的列表:

1. 选择您要检查的计算机所在的组。

2. 在 **查看** 下拉列表中，选择您想要显示的计算机，例如，**有潜在问题的计算机**。



您还可以选择此项下的子项，以显示被特定的问题影响的计算机（如：与组策略不一致的计算机，具有未处置的警报的计算机，或者，出现安装错误的计算机）。

3. 如果该组含有子组，请选择您是 **仅在这一级** 或在 **在这一级，及以下级**。

   任何保护有问题的计算机，都将被列示出来。

要了解处置保护问题的信息，请参见“排疑解难”部分。

11 处置警报和错误

11.1 警报图标的含义

如果有病毒，间谍软件，可疑项目，广告软件，或其它可能不想安装的应用程序，警告图标会出现在 **终结点** 视图的 **状态** 标签页中。

以下是警报图标的示例。在本节的其它主题中，您可以找到针对这些警报的相关建议。

注: 如果软件已禁用，或者未及时更新，在控制台中也会出现警告信息。要了解相关信息，请参见 怎样检查网络是否受到保护？（第44页）。

警报图标

图标	释意
(红色警报图标)	出现在 **警报和错误** 栏中的红色警报标志表明，检测到了病毒，蠕虫，特洛伊，间谍软件，或可疑行为。
(黄色警告图标)	出现在 **警报和错误** 栏中的黄色警告标志表明，以下情况之一: ■ 检测到了可疑文件。 ■ 检测到了广告软件或其它可能不想安装的应用程序。 ■ 出现错误。 出现在 **策略遵照** 栏中的黄色警告标志表明，该计算机没有使用与它所在的组中的其它计算机使用的策略相同的策略。

如果计算机中出现了多个警报和错误，具有最高的优先级的警报的图标，会出现 **警报和错误** 栏中。以下列示的警报类型，以降序排列优先级。

1. 病毒和间谍软件警报
2. 可疑行为警报
3. 可疑文件警报
4. 广告软件和可能不想安装的应用程序 (PUA) 警报
5. 软件应用程序错误（例如，安装错误）

要了解更多有关某个警报的详情，例如，检测到的项目的名称，请单击**警报和错误详情** 标签页。

11.2 处置警报

如果您使用基于角色的管理，您必须具备 **调整-清除** 权限，才能从控制台清除检测到的项目，或者清除警报。要了解更多信息，请参见 关于角色和子领域（第11页）。

要针对在控制台中显示的警报采取措施:

1. 在 **终结点** 视图中，选择您想要查看警报的计算机。右击并选择 **处置警报和错误**。

   会出现 **处置警报和错误** 对话框。

2. 针对警报您可以采取的措施，取决于警报的清除状态。查看 **清除状态** 栏目，并决定您要采取什么措施。

提示: 您可以单击栏标排序警报。例如，要按照清除状态排序警报，请单击 **清除状态** 栏标。

清除状态	描述和采取的措施
可清除	您可以删除该项目。要这样做，请勾选一个或多个警报，并单击**清除**。
不能清除的安全隐患类型	这一类型的检测到的项目，例如：可疑文件，或可疑行为，无法通过控制台中清除它们。您只能决定允许或阻断该项目。如果您不信任该项目，您可以将它发送给 Sophos 进行分析。要了解更多信息，请参见 查找检测到的项目的信息（第52页）。
不可清除	此项目无法通过控制台清除。要了解更多有关此项目的信息，以及您可以采取的措施，请参见 查找检测到的项目的信息（第52页）。
要求完整扫描	此项目可能可以清除，但是需要对终结点计算机进行完整扫描，才能进行清除工作。要了解操作指导，请参见 现在扫描计算机（第62页）。
要求重新启动	该项目已部分地被删除，但是终结点计算机需要重新启动，以完成清除工作。 **注:** 必须从本地，而不是从 Enterprise Console 中，重新启动终结点计算机。
清除失败	该项目不能被删除。要求手动清除。要了解更多信息，请参见 处置清除失败的已检测到的项目（第54页）。
清除正在进行中（启动 <时间>）	清除正在进行。
清除超时（启动 <时间>）	清除已超时。该项目可能没有被清除。这可能发生在，例如，终结点计算机与网络的连接断开，或网络繁忙时。您可以稍后在尝试清除项目。

如果您决定批准项目，请参见 批准广告软件和可能不想安装的应用程序（第84页） 或 批准可疑项目（第80页）。

11.3 查找检测到的项目的信息

如果您想要了解更多有关安全隐患或终结点计算机上检测到，并在控制台中报告的项目的信息，或者，需要有关针对该项目应该采取何种措施的建议，请按照以下步骤做:

1. 在 **终结点** 视图的计算机列表中，双击有关的计算机。

2. 在 **计算机详情** 对话框中，拖动滚动条找到 **未处置的警报和错误** 部分。 在已检测到的项目列表中，单击您想要相关的项目名称。

   这会将链接到 Sophos 网站，您可以在那里阅读项目的描述，有关针对该项目应该采取何种措施的建议

注: 或者，您可以访问 Sophos 网站上的 **安全分析** 页面。(*(http://cn.sophos.com/security/analyses/*)，在您想要查找的项目类型的标签页中，在搜索栏中输入项目的名称，或者，在项目列表中查找项目。

11.4 从控制台清除终结点计算机的警报或错误

如果您使用基于角色的管理，您必须具备 **调整-清除** 权限，才能从控制台清除警报或错误。 要了解更多信息，请参见 关于角色和子领域（第11页）。

如果您正在处置警报，或者，您确信发出警报的计算机是安全的，您可以清除显示在控制台中的警报标志。

注: 您无法清除有关安装错误的警报。 只有在计算机上顺利安装了 Sophos Endpoint Security and Control，您才能清除它们。

1. 在 **终结点** 视图中，选择您想要清除警报的计算机。 右击并选择 **处置警报和错误**。

   会出现 **处置警报和错误** 对话框。

2. 要从控制台中清除警报或 Sophos 产品的错误，请相应地转到“警报”或“错误”标签页中，选择您想要清除的警报或错误，然后，单击 **确认已知**。

   确认已知的（清空的）警报不再出现在控制台中。

要了解更多有关从控制台清除更新管理器警报的信息，请参见 从控制台中清除更新管理器警报（第53页）。

11.5 从控制台中清除更新管理器警报

如果您使用基于角色的管理，您必须具备 **调整-清除** 权限，才能从控制台清除警报。 要了解更多信息，请参见 关于角色和子领域（第11页）。

要从控制台中清除更新管理器警报:

1. 在 **更新管理器** 视图中，选择您想要清除警报的更新管理器。 单击鼠标右键，并选择 **确认已知警报**。

   会出现 **更新管理器警报** 对话框。

2. 要从控制台清除警报，请选择您想要清除的警报，然后，单击 **确认已知**。

   确认已知的（清空的）警报不再出现在控制台中。

12 清除计算机

12.1 立即清除计算机

您可以立即清除 Windows 2000 及以后的计算机中的病毒，或者，不想安装的程序。

如果您使用基于角色的管理，您必须具备 **调整-清除** 权限，才能清除计算机。要了解更多信息，请参见 关于角色和子领域（第11页）。

注: 要清除 Windows 95/98/NT4，Mac，Linux 或 UNIX 计算机，您既可以从控制台（参见 设置自动清除（第55页）），也可以按照 处置清除失败的已检测到的项目（第54页）中的说明，个别地清除计算机。

如果某个项目（例如，特洛伊木马或可能不想安装的应用程序）被“部分地检测到”，那么，在清除受到影响的计算机之前，您需要对该计算机进行完整系统扫描，找到该“部分地检测到”的项目的所有组件。在计算机列表的 **终结点** 视图中，右击受到影响的计算机，并单击 **完整系统扫描**。要了解更多信息，请参见 部分检测到项目（第177页）。

要立即清除计算机:

1. 在计算机列表的 **终结点** 视图中，右击您想要清除的计算机，并单击view, right-click the computer(s) that you want to clean up and then click **处置警报和错误**。
2. 在 **处置警报和错误** 对话框的 **警报** 标签页中，选择您想要清除的各个项目，或者，单击 **全选**。单击 **清除**。

如果清除成功，在计算机列表中出现的警报会消失。

如果还有警报剩下，您应该进行手动清除计算机。请参见 处置清除失败的已检测到的项目（第54页）。

12.2 处置清除失败的已检测到的项目

如果您无法从控制台中清除计算机中的安全隐患，您可以进行手动清除。

1. 在计算机列表中，双击被感染的计算机。

2. 在 **计算机详情** 对话框中，拖动滚动条找到 **未处置的警报和错误** 部分。 在已检测到的项目列表中，单击您想要从计算机中删除的项目名称。

   这将连接到 Sophos 网站，您可以在那里阅读这样清除计算机的建议。

3. 转到该计算机上，进行手动清除的工作。

   注: Sophos 的网站可提供一些特别针对某些病毒和蠕虫的可下载的清除病毒小程序。

12.3 设置自动清除

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以在一旦发现病毒或其它项目时，就立即自动清除计算机。 要这样做，您可以按照以下说明更改读写扫描和计划扫描。

注: 读写扫描不能够清除的广告软件和可能不想安装的应用程序(PUA)。 您应该按照 立即清除计算机（第54页） 中的说明，处置它们。或者，在计划扫描中启用自动清除广告软件和可能不想安装的应用程序。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。

2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。 然后，双击您想要更改的策略。

   会出现 **防病毒和 HIPS 策略** 对话框。

3. 为读写扫描设置自动清除。

   在 **配置防病毒和 HIPS** 面板中，单击 **读写扫描** 按钮。 在 **读写扫描设置** 对话框中，单击 **清除** 标签。 请按以下说明设置选项。

   病毒 / 间谍软件

   选择 **自动清除项目中的病毒 / 间谍软件**。 您还可以指定如果清除失败，应该处置这些项目。

   - 仅拒绝访问（默认值）
   - 删除
   - 拒绝访问并移至默认的路径
   - 拒绝访问并移至 <指定的 UNC 路径>

   注: 任何这些设置都不应用于 Windows 95/98 计算机。

   即使您选择了 **拒绝访问并移至** 并指定了路径，Mac OS X 计算机仍然会将文件移至默认的路径。
   拒绝访问并移至默认的路径 和 **拒绝访问并移至** 的设置不应用于 Linux 和 UNIX 计算机，这些计算机将忽略这两种设置。

   可疑文件

   注: “可疑文件”设置仅应用于 Windows 2000 及以后的计算机。

   您可以指定如果检测到了可疑文件，应该处置它们。

   - 仅拒绝访问（默认值）
   - 删除
   - 拒绝访问并移至默认的路径
   - 拒绝访问并移至 <指定的 UNC 路径>

4. 为计划扫描设置自动清除。

   在 **防病毒和 HIPS 策略** 对话框的 **计划扫描** 面板中，选中该扫描，然后单击 **编辑**。 然后，在 **计划扫描设置** 对话框中，单击 **配置**。 在 **扫描和清除设置** 对话框中，单击 **清除** 标签。 请按以下说明设置选项。

   病毒 / 间谍软件

   选择 **自动清除项目中的病毒 / 间谍软件**。 您还可以指定如果清除失败，应该处置这些项目。

   - 仅拒绝访问（默认值）
   - 删除
   - 拒绝访问并移至默认的路径
   - 拒绝访问并移至 <指定的 UNC 路径>

   注: 即使您选择了 **拒绝访问并移至** 并指定了路径，Windows 95/98 计算机仍然会将文件移至默认的路径。

   广告软件和可能不想安装的应用程序 (PUA)

   如果您想要，请选择 **自动清除广告软件和可能不想安装的应用程序**。

   注: “广告软件和可能不想安装的应用程序”设置仅应用于 Windows 2000 及以后的计算机。

   可疑文件

   注: “可疑文件”设置仅应用于 Windows 2000 及以后的计算机。

   您可以指定如果检测到了可疑文件，应该处置它们。

   - 仅拒绝访问（默认值）
   - 删除
   - 拒绝访问并移至默认的路径
   - 拒绝访问并移至 <指定的 UNC 路径>

13 查看事件

13.1 关于事件

当某终结点计算机上出现应用程序控制，防火墙，数据控制，或设备控制事件时，例如，某应用程序已被防火墙阻断，该事件会被发送到 Enterprise Console，并且可以在相应的事件查看器中被查看。

通过事件查看器，您可以调查发生在网络中的事件。您还可以基于您配置的过滤器生成事件列表，例如，某用户在过去7天中发生的所有数据控制事件的列表。

在最近七日之内，发生事件的数量超过了指定的级别的计算机，会显示在指标面板中。要了解怎样设置级别的信息，请参见配置指标面板（第47页）。

您还可以设置当发生事件时，向您选择的收件人发送警报。要了解更多信息，请参见“设置警报”部分。

13.2 查看应用程序控制事件

要查看应用程序控制事件:

1. 在 **查看** 菜单中，单击 **应用程序控制事件**。

   会出现 **应用程序控制 - 事件查看器** 对话框。

2. 在 **搜索时间跨度** 栏中，单击下拉箭头，并选择您想要显示的事件所在的时间跨度。

   您可以选择固定的时间跨度，如：**24 小时内**，或者，选择 **自定义**，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。

3. 如果您想查看某个用户或计算机的事件，请在相应的栏中输入名称。

   如果您保留这些栏为空，那么，将显示所有用户和计算机的事件。

   您在这些栏中使用通配符。使用 ? 替代单个字符，以及使用 * 替代字符串。

4. 如果您想查看某个应用程序类型的事件，请单击 **应用程序类型** 栏上的下拉菜单，并选择应用程序类型。

   依照默认值，事件查看器会显示所有应用程序类型的事件。

5. 单击 **搜索** 可显示事件列表。

您可以将应用程序控制事件列表导出到文件中。要了解详情，请参见导出事件列表到文件中（第61页）。

13.3 查看数据控制事件

要查看数据控制事件:

1. 在 **查看** 菜单中，单击 **数据控制事件**。

   会出现 **数据控制 - 事件查看器** 对话框。

2. 在 **搜索时间跨度** 栏中，单击下拉箭头，并选择您想要显示的事件所在的时间跨度。

   您可以选择固定的时间跨度，如：**24 小时内**，或者，选择 **自定义**，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。

3. 如果您想查看某个用户，计算机，或者，文件，请在相应的栏中输入名称。

   如果您保留这些栏为空，那么，将显示所有用户，计算机，和文件的事件。

   您在这些栏中使用通配符。 使用 ? 替代单个字符，以及使用 * 替代字符串。

4. 如果您想要查看针对某个规则的事件，请在 **规则名称** 栏，单击下拉箭头，并选择规则名称。

   依照默认值，事件查看器会显示针对所有规则的事件。

5. 如果您想查看某个文件类型的事件，请在 **文件类型** 栏中，单击下拉箭头，并选择文件类型。

   依照默认值，事件查看器会显示所有文件类型的事件。

6. 单击 **搜索** 可显示事件列表。

您可以将数据控制事件列表导出到文件中。 要了解详情，请参见 导出事件列表到文件中（第61页）。

13.4 查看设备控制事件

要查看设备控制事件:

1. 在 **查看** 菜单中，单击 **设备控制事件**。

   会出现 **设备控制 - 事件查看器** 对话框。

2. 在 **搜索时间跨度** 栏中，单击下拉箭头，并选择您想要显示的事件所在的时间跨度。

   您可以选择固定的时间跨度，如：**24 小时内**，或者，选择 **自定义**，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。

3. 如果您想查看某个设备类型的事件，请在 **设备类型** 栏中，单击下拉箭头，并选择设备类型。

   依照默认值，事件查看器会显示所有设备类型的事件。

4. 如果您想查看某个用户或计算机的事件，请在相应的栏中输入名称。

   如果您保留这些栏为空，那么，将显示所有用户和计算机的事件。

   您在这些栏中使用通配符。 使用 ? 替代单个字符，以及使用 * 替代字符串。

5. 单击 **搜索** 可显示事件列表。

在 **设备控制 - 事件查看器** 对话框中，您可以从设备控制策略中免除设备。 要了解详情，请参见 从所有策略中免除设备（第143页）。

您可以将设备控制事件列表导出到文件中。 要了解详情，请参见 导出事件列表到文件中（第61页）。

13.5 查看防火墙事件

防火墙事件从终结点计算机到控制台只发送一次。来自不同的终结点计算机的相同的事件，在 **防火墙 - 事件查看器** 中会被放置在一起。 在 **计数** 栏中，您可以看到某个事件被从不同的终结点计算机发送出来的总次数。

要查看防火墙事件:

1. 在 **查看** 菜单中，单击 **防火墙事件**。

   会出现 **防火墙 - 事件查看器** 对话框。

2. 在 **搜索时间跨度** 栏中，单击下拉箭头，并选择您想要显示的事件所在的时间跨度。

   您可以选择固定的时间跨度，如: **24 小时内**，或者，选择 **自定义**，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。

3. 如果您想查看某个类型的事件，请在 **事件类型** 栏中，单击下拉箭头，并选择事件类型。

   依照默认值，事件类型查看器会显示所有类型的事件。

4. 如果您想查看某个文件的事件，请在 **文件名** 栏中，输入文件名称。

   如果您保留此栏为空，所有文件的事件都会显示。

   您可以在此栏中使用通配符。 使用 ? 替代单个字符，以及使用 * 替代字符串。

5. 单击 **搜索** 可显示事件列表。

在 **防火墙 - 事件浏览器** 对话框中，您可以按照 创建防火墙规则（第116页）中的说明创建防火墙规则。

您可以将防火墙事件列表导出到文件中。 要了解详情，请参见 导出事件列表到文件中（第61页）。

13.6 查看介入防范事件

介入防范事件有两种类型:

- 顺利的介入防范验证事件，显示已验证的用户的名称，以及验证的时间。

- 不成功的介入尝试事件，显示涉及的 Sophos 软件产品或组件的名称，介入尝试的时间，以及进行介入尝试的用户的详情。

要查看介入防范事件:

1. 在 **查看** 菜单，单击 **介入防范事件**。

   会出现 **介入防范 - 事件查看器** 对话框。

2. 在 **搜索时间跨度** 栏中，单击下拉箭头，并选择您想要显示的事件所在的时间跨度。

   您可以选择固定的时间跨度，如：**24 小时内**，或者，选择 **自定义**，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。

3. 如果您想要查看某个类型的事件，请在 **事件类型** 栏中，单击下拉箭头，并选择事件类型。

   依照默认值，事件查看器会显示所有类型的事件。By default, the event viewer displays events of all types.

4. 如果您想查看某个用户或计算机的事件，请在相应的栏中输入名称。

   如果您保留这些栏为空，那么，将显示所有用户和计算机的事件。

   您在这些栏中使用通配符。使用 ? 替代单个字符，以及使用 * 替代字符串。

5. 单击 **搜索** 可显示事件列表。

您可以将此列表导出到文件中。要了解详情，请参见 导出事件列表到文件中（第61页）。

13.7 查看被阻断的网站

您可以查看最近在某个终结点计算机上被阻断的网站的名单。

要查看最近被阻断的网站:

1. 在 **终结点** 视图的计算机列表中，双击您想要查看被阻断的网站的计算机。
2. 在 **计算机详情** 对话框中，下拉滚动条到 **最近阻断的网站** 部分。

您还可以通过生成报告查看某个用户的被阻断的网站的数量。要了解更多信息，请参见 配置每个用户的事件的报告（第166页）。

13.8 导出事件列表到文件中

您可以导出应用程序控制，防火墙，数据控制，或设备控制事件列表到某个逗号分隔值 (csv) 文件中。

1. 在 **查看** 菜单中，根据您想要导出的某种事件列表，单击该种“事件”选项。

   事件查看器 对话框会出现。

2. 如果您只想查看特定的事件，请在 **搜索标准** 窗格板中，设置合适的筛选项，然后，单击 **搜索** 按钮，以显示事件。

   要了解更多信息，请参见 查看应用程序控制事件（第58页），查看数据控制事件（第58页），查看设备控制事件（第59页），或 查看防火墙事件（第60页）。

3. 单击 **导出**。
4. 在 **另存为** 对话框中，输入文件名，并浏览找到为文件所选择的目标文件夹。

14 扫描计算机

14.1 关于扫描

依照默认值，在用户试图访问带有已知的和未知的病毒，特洛伊木马，蠕虫，以及间谍软件的文件时，Sophos Endpoint Security and Control 可以自动检测到它们。 它还可以分析正在系统中运行的程序的行为。

您还可以配置 Sophos Endpoint Security and Control 进行以下工作:

- 扫描计算机中的可疑文件。 请参见 扫描可疑文件（第79页）。
- 扫描广告软件和其它可能不想安装的应用程序。 请参见 扫描广告软件和可能不想安装的应用程序（第83页）。
- 在设定的时间扫描计算机。 请参见 在设定的时间扫描计算机（第92页）。

要了解更多有关配置扫描的信息，请参见“配置防病毒和 HIPS 策略”部分。

本节说明怎样立即在所选择的计算机上执行完整系统扫描。

14.2 现在扫描计算机

您可以立即扫描一个或数个计算机，无需等到下一次的计划扫描。

如果您使用基于角色的管理，您必须具备 **调整-更新和扫描** 权限，才能扫描计算机。 要了解更多信息，请参见 关于角色和子领域（第11页）。

注: 只有 Windows 2000 或以后的计算机，以及 UNIX 计算机，可以执行从控制台启动的即时完整系统扫描。

要即时扫描计算机:

1. 请选择计算机列表中的计算机，或窗格板中的 **组**。 右击并选择 **完整系统扫描**。

   或者，在 **措施** 菜单中，选择 **完整系统扫描**。

2. 在 **完整系统扫描** 对话框中，查看将要被扫描的计算机的详情，然后，单击 **确定** 以启动扫描。

15 更新计算机

15.1 更新未及时更新的计算机

如果您使用基于角色的管理，您必须具备 **调整-更新和扫描** 权限，才能更新计算机。 要了解更多信息，请参见 关于角色和子领域 （第11页）。

在您设置了更新策略，并将它们应用到联网计算机之后，计算机会自动保持更新。 除非更新出现问题，您不必手动更新计算机。

如果在 **终结点** 视图的计算机列表中，您看到 **状态** 标签页的 **更新情况** 栏中的计算机旁出现一个时钟图标，则表明该计算机未及时更新计算机软件。 旁边的文字，说明是该计算机已有多长时间没有及时更新了。

计算机可能由于以下两个原因之一，而未及时更新:

- 该计算机从服务器获取更新文件失败。
- 供更新所用的服务器中不是最新的 Sophos 软件。

要诊断问题并更新计算机。

1. 在 **终结点** 视图中，选择含有未及时更新的计算机的组。
2. 在 **状态** 标签页中，单击 **更新情况** 栏标，将计算机按照更新情况排序。
3. 单击 **更新详情** 标签，并查看 **主服务器** 栏。

   在该栏中会向您显示各计算机从中更新的目录。

4. 现在，查看从某一特定目录中更新的所有计算机。
   - 如果其中有一些计算机已及时更新，而另外一些却没有，那么，是个别的计算机有问题。选择它们，单击鼠标右键，并单击 **立即更新计算机**。
   - 如果所有的计算机都未及时更新，那么，可能是供更新的目录有问题。在 **视图** 菜单中，单击 **更新管理器**。选择维护您认为未及时更新的那个路径的更新管理器，单击鼠标右键，并单击 **立即更新**。然后在 **视图** 菜单中，单击 **终结点**。选择未及时更新的计算机，单击鼠标右键，并单击 **立即更新计算机**。

   如果您具有多个更新管理器，而不清楚哪个更新管理器维护未及时更新的路径，请使用“更新层级”报告，查看各个更新管理器维护的是哪些共享文件夹。要查看“更新层级”报告，请在 **工具** 菜单中，单击 **管理报告**。在 **报告管理器** 对话框中，选择 **更新层级** 并单击 **运行**。查看报告中的“由更新管理器管理的共享”部分。

16 配置软件预订

16.1 关于软件预订

软件预订指定从 Sophos 为各操作平台的计算机下载哪个版本的终结点软件。

下载安全软件向导 可以设置一个名为“建议”的软件预订。该软件预订包括任何所选的软件的建议版本。

如果您想预订不是建议版的版本，请按照 预订安全软件（第65页） 中的说明配置预订。

如果您在安装 Enterprise Console 了之后，没有结束此向导，请参见 运行下载安全软件向导（第66页）。

16.2 什么类型的更新文件可供使用?

对于每个主要版本的解决方案（如：Sophos Endpoint Security and Control 9）和操作平台（如：Windows 2000 或以后）都有数个版本的软件相关联。通过在软件预订中选择更新文件类型，您可以选择从 Sophos 下载的，将要部署到终结点计算机中的软件版本。您可以在三种标记和三种固定的软件版本中进行选择。

标记版本

有三种标记版本:

标记	描述
建议	此版本 Sophos 认为最适合需要最及时更新的产品的用户。 Sophos 通常建议尽快将发布的最新板的终结点软件部署到终结点计算机中。
先前	当前版本之前的建议版本。
最早	Sophos 仍然提供更新支持的最早的版本。

注: Sophos 也许会在将来添加新的标记版本。

下载安全软件向导 可以设置软件预订，指定任何所选的软件的建议版本。

当预订了标志版本后，如：“建议”或“先前”，Enterprise Console 将总是从 Sophos 下载相应标志的版本。 实际所下载的版本通常每个月会有所不同。

固定版本

固定版本随新的安全隐患数据而更新，而不是随每个月的最新软件版本而更新。

如果您想要在将新版本的软件部署到网络中之前，评估使用它们，那么，您可以考虑在评估使用新版本的软件的时候，在网络中使用该软件的固定版本。

通常，针对每个操作系统有三种固定版本，对应最近三个月来，每个月所发布的版本。 一个固定版本的例子是：Sophos Endpoint Security and Control for Windows 2000 及以后，版本 9.4.3。

只要 Sophos 提供了固定版本，就可以随时下载它。 如果某个固定的版本将要被淘汰，您会在任何下载该版本的更新管理器旁的 **更新管理器** 视图中看到相关的警报。 如果您配置了电子邮件警报发送，管理员还会收到相关的电子邮件警报。

依照默认值，如果某个一直在某软件预订中使用的固定版本被淘汰了，那么，Enterprise Console 将重新定义软件预订使用仍然提供的最早的那个固定版本。

注: 您可以通过取消勾选 **当出现 Sophos 不再支持的固定版软件时，自动升级该固定版软件** 勾选框，在预订中进行更改。 不过，请注意运行不再支持的软件，会使您无法受到针对新的安全隐患而提供的保护。 因此，Sophos 建议您尽快升级不再支持的版本。

16.3 预订安全软件

如果您使用基于角色的管理，那么，：

- 您必须具有 **策略设置 - 更新** 权限，才能编辑软件预订。

- 如果某个软件预订所应用的更新策略是被应用到您的活动子领域之外的，那么，您不能编辑该软件预订。

要了解更多有关基于角色的管理的信息，请参见关于角色和子领域 (第11页)。

要预订安全软件:

1. 在 **视图** 菜单中，单击 **更新管理器**。
2. 在 **软件预订** 窗格板中，双击您想要更改的预订，或单击窗格板顶部的 **添加** 按钮，以创建新的预订。

   会出现 **软件预订** 对话框。

   或者，如果您想要复制一份现有的预订，请选择该预订，单击鼠标右键，然后单击 **复制预订**。 为预订输入新的名称，然后，双击它，打开 **软件预订** 对话框。
3. 在 **软件预订** 对话框中，如果您想要，可以编辑软件预订的名称。
4. 选择您想要下载软件的操作平台。

   重要: 如果您想下载 Sophos Anti-Virus for NetWare，请阅读 Sophos 技术支持知识库文章 59192 (*http://cn.sophos.com/support/knowledgebase/article/59192.html*)。
5. 针对各所选的操作平台，单击操作平台旁的**版本**栏，然后，再次单击。 在可用版本的下拉菜单中，选择您想要下载的版本。

   通常，您要预订 "建议" 版本，以确保您的软件自动保持及时更新。 要了解其它可以使用的更新类型，请参见 什么类型的更新文件可供使用? (第64页)

   重要: 如果选择了固定版本，例如，9.1.2，那么，Sophos 建议您保留勾选 **当出现 Sophos 不再支持的固定版软件时，自动升级该固定版软件**。 勾选框。 运行不再支持的软件，将使您无法防范新出现的安全隐患。

在预定了安全软件之后，您可以设置软件预订的电子邮件警报。 要了解更多有关软件预订的电子邮件警报的信息，请参见 设置软件预订警报 (第151页)。

如果您创建了新的软件预订，请按照 查看或编辑更新管理器配置 (第67页) 中的说明配置更新管理器以维护它。

16.4 运行下载安全软件向导

如果您使用基于角色的管理，您必须具备 **策略设置 - 更新** 权限，才能运行 **下载安全软件向导**。 要了解更多信息，请参见 关于角色和子领域 (第11页)。

如果您在安装了 Enterprise Console 了之后，尚未完成 **下载安全软件向导**，请按照以下说明做:

- 在 **措施** 菜单中，单击 **运行下载计算机软件向导**。

  下载安全软件向导 会指导您完成选择和下载软件。

16.5 查看哪个更新策略使用软件预订

要查看哪个更新策略使用了特定的软件预订:

- 选择预订，单击鼠标右键，然后，单击 **查看用法**。

  在 **软件预订用法** 对话框中，您可以看到使用软件预订的更新策略的列表。

17 配置更新管理器

17.1 什么是更新管理器?

更新管理器使您能够设置从 Sophos 网站自动更新 Sophos 安全软件。 更新管理器与 Enterprise Console 安装在一起，并由 Enterprise Console 管理。

您可以安装多个更新管理器。例如，如果您具有带有数个路径的复杂网络，您可能想在远程路径中安装附加的更新管理器。 要了解信息，请参见 添加附加的更新管理器（第74页）。

17.2 更新管理器怎样工作?

一旦您配置了更新管理器，它会:

- 定时连接 Sophos 或您的网络中的数据分发仓库。
- 下载更新文件到安全隐患检测数据，以及下载系统管理员预订的安全软件的更新文件。
- 以适合在终结点计算机进行安装的形式，将更新后的软件放置到一个或多个网络共享中。

计算机会自动从共享文件夹中进行更新，只要安装在这些计算机上 Sophos 软件已经 — 例如，通过应用更新策略，— 进行了这样的配置。

17.3 查看或编辑更新管理器配置

如果您使用基于角色的管理，您必须具有 **策略设置 - 更新** 权限，才能配置更新管理器。 要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 如果您在 **终结点** 视图中，单击工具栏上的 **更新管理器** 按钮，以显示 **更新管理器** 视图。
2. 在更新管理器列表中，选择您想要查看或编辑其配置的更新管理器。 单击鼠标右键，并单击 **查看/编辑配置**。

   注: 或者，选择更新管理器，转到 **措施** 菜单，指向 **更新管理器**，然后，单击 **查看/编辑配置**。

   会出现 **配置更新管理器** 对话框。

3. 按照以下主题中的说明，编辑配置:
   - 为更新管理器选择更新源 (第68页).
   - 选择要下载的软件 (第69页).
   - 指定在何处放置软件 (第70页).
   - 创建或编辑更新计划 (第72页).
   - 配置更新管理器日志记录 (第72页).
   - 配置更新管理器更新自身 (第73页).

要了解更多有关从控制台清除更新管理器警报的信息，请参见从控制台中清除更新管理器警报 (第53页)。

在您配置了更新管理器之后，您可以配置更新策略，并将它们应用到终结点计算机上。

17.4 为更新管理器选择更新源

如果您使用基于角色的管理，您必须具有 **策略设置-更新** 权限，才能配置更新管理器。 要了解更多信息，请参见 关于角色和子领域 (第11页)。

您需要选择一个更新源，更新管理器将从那里下载安全软件和更新文件，以将它们分发到网络中。

您可以选择数个更新源。 列表中的第一个更新源是主更新源。 列表中附加的更新源，是可选的备用路径，以备更新管理器无法从主更新源获取更新文件时使用。

1. 如果您在 **终结点** 视图中，单击工具栏上的 **更新管理器** 按钮，以显示 **更新管理器** 视图。
2. 在更新管理器列表中，选择您想要为其选择更新源的更新管理器。 单击鼠标右键，并单击 **查看/编辑配置**。

3. 在 **配置更新管理器** 对话框中的 **更新源** 标签页中，单击 **添加**。
4. 在 **更新源详情** 对话框中的 **地址** 栏中，输入更新源地址。该地址可以是 UNC 或 HTTP 路径。

   如果您想要直接从 Sophos 下载软件和更新文件，请选择 **Sophos**。
5. 如果需要，可在 **用户名** 和 **密码** 栏中，输入将要用来访问更新源的帐户的用户名和密码。
   - 如果更新源是 Sophos，请输入由 Sophos 提供的下载认证资料。
   - 如果更新源是由位于较高的更新层级中的更新管理器创建默认更新共享，那么，**用户名** 和 **密码** 栏会被事先输入。

     默认的更新共享，是一个 UNC 共享：\\<计算机名>\SophosUpdate，这里的“计算机名”是更新管理器安装所在的计算机的名称。
   - 如果更新共享不是您的网络中默认的更新共享，请输入对网络共享具备读权限的认证资料。如果 **用户名** 需要指明域，才算合格有效，请使用“域\用户名”的形式。
6. 如果您通过代理服务器访问更新源，那么，请选择 **使用代理服务器连接**。然后，输入代理服务器的 **地址** 和 **端口** 号。输入用来接入代理服务器的 **用户名** 和 **密码**。如果“用户名”需要指明域，才算合格有效。请使用“域\用户名”的形式。单击 确定。

   新的更新源会出现在 **配置更新管理器** 对话框中的列表里。

如果您已在不同的计算机上安装了更新管理器，那么，该更新管理器从中下载软件和更新文件的共享文件夹将出现在地址列表中。您可以选择该共享文件夹作为您正在配置的更新管理器的更新源。然后，使用列表右侧的 **上移** 或 **下移** 按钮，您可以将想要作为主更新源的地址移动到列表的最上方。

17.5 选择要下载的软件

如果您使用基于角色的管理，您必须具有 **策略设置 - 更新** 权限，才能配置更新管理器。要了解更多信息，请参见 关于角色和子领域（第11页）。

您需要为更新管理器选择将保持及时更新的软件预订。

1. 如果您在 **终结点** 视图中，单击工具栏上的 **更新管理器** 按钮，以显示 **更新管理器** 视图。
2. 在更新管理器列表中，选择您想要为其选择下载的软件的更新管理器。单击鼠标右键，并单击 **查看/编辑配置**。

3. 在 **配置更新管理器** 对话框的 **预订** 标签页中，从可用的软件预订列表中选择软件预订。

   要查看软件预订详情，如：软件预订中包括什么软件，请单击 **查看详情**。

4. 要将所选的软件预订移动到“已预订”列表中，请单击“添加”按钮。

   要将所有的软件预订移动到“已预订”列表中，请单击“全部添加”按钮。

17.6 指定在何处放置软件

如果您使用基于角色的管理，您必须具有 **策略设置 - 更新** 权限，才能配置更新管理器。 要了解更多信息，请参见 关于角色和子领域（第11页）。

在您选择要下载的软件后，您可以指定在网络中的何处放置它。依照默认值，软件将放置在 UNC 共享文件夹 \\<计算机名>\SophosUpdate 中，这里的“计算机名”是更新管理器安装所在的计算机。

您可以将已下载的软件分发到网络中的附加的共享中。 要这样做，请将现有的网络共享添加到可用共享列表中，然后，按照以下说明，将它移动到更新共享列表中。 请确保 **SophosUpdateMgr** 帐户对这些共享具有对权限。

要了解支持网络共享的操作平台列表，请参见 网络共享支持什么操作平台？（第71页）

要指定在何处放置软件：

1. 如果您在 **终结点** 视图中，单击工具栏上的 **更新管理器** 按钮，以显示 **更新管理器** 视图。
2. 在更新管理器列表中，选择您想要为其选择用来分发软件的网络共享的更新管理器。 单击鼠标右键，并单击 **查看/编辑配置**。
3. 在 **配置更新管理器** 对话框的 **分发** 标签页中，从列表中选择软件预订。

4. 从“可用”共享列表中选择一个共享文件夹，并单击“添加”按钮(>)，将它移到“更新至”列表中。

   默认的共享 \\<计算机名>\SophosUpdate 总是会出现在“更新至”列表中。您无法从列表中删除此共享。

   “可用”共享列表包括 Enterprise Console 所有已知的共享，尚未被其它更新管理器使用的共享。

   您可以使用“添加”(>)或“删除”(<)按钮，添加现有的共享到“可用”共享列表，或者，从“可用”共享列表中删除共享。

5. 如果您想要输入共享描述，或者，输入写访问共享所需的认证资料，请选择该共享，并单击 **配置**。 在 **共享管理器** 对话框中，输入描述和认证资料。

   如果您想为多个共享输入同样的认证资料，请在“更新到”列表中选择这些共享，并单击 **配置**。 在 **配置多个共享** 对话框中，输入写访问所需要的认证资料。

17.7 网络共享支持什么操作平台？

以下操作平台支持网络共享:

- 在 Windows NT 及以后上的共享。
- Linux 服务器（如，SUSE Linux Enterprise 10 (SLES 10)）上的 Samba 共享，
- Netware 5.1 SP3 和 Netware 6.5 SP3 to SP7，Netware kernel 上的 Samba 共享。
- Mac OSX 10.2 或以后上的 Samba 共享。
- Unix 上的 Samba 共享。
- Novell Open Enterprise Server 1/2，Linux kernel 上的 Novell Storage Services (NSS) ，支持 NDS 身份验证的。
- Netware 5.1 SP3 和 Netware 6.5 SP3-SP7，Netware kernel 上的 Netware File System (NFS) 共享，支持 NDS 身份验证。
- NetApp Filer。
- Novell Open Enterprise Server 1/2 上的 Samba 共享。
- Netware 5.1 SP3 和 Netware 6.5 SP3-SP7，Netware kernel 上的 Novell Storage Services (NSS) 共享，支持 NDS 身份验证。

17.8 创建或编辑更新计划

如果您使用基于角色的管理，您必须具有 **策略设置 - 更新** 权限，才能配置更新管理器。 要了解更多信息，请参见 关于角色和子领域（第11页）。

依照默认值，更新管理器会每隔10分钟检查一次安全隐患检测数据更新文件。 您可以更改此更新频率。 最小值是 5 分钟。 最大值是 1440 分钟（24 小时）。 Sophos 建议每隔 10 分钟做一次安全隐患检测数据更新检查，这样，您可以在 Sophos 发布检测数据后，立即就接收到最新的安全隐患保护。

依照默认值，更新管理器会每隔 60 分钟检查一次软件更新文件。 您可以更改此更新频率。 最小值是 10 分钟。 最大值是 1440 分钟（24 小时）。

对于软件更新文件，您既可以指定某个频率，在每天的每个小时中使用，也可以创建一个更周密的计划，具体指定每周各天中的更新频率，以及在各天中的不同时段，使用不同的更新频率。

注: 您可以为每周中的各天创建不同的计划 每周中的各天只能于一个计划关联。

1. 如果您在 **终结点** 视图中，单击工具栏上的 **更新管理器** 按钮，以显示 **更新管理器** 视图。
2. 在更新管理器列表中，选择您想要为其创建更新计划的更新管理器。 单击鼠标右键，并单击 **查看/编辑配置**。
3. 在 **配置更新管理器** 对话框中的 **计划** 标签页中，输入检查安全隐患检测数据更新文件的频率。
4. 输入检查软件更新文件的频率。
   - 如果您想指定在每天的每个小时中使用的更新频率，请选择 **每 n 分钟检查一次更新文件** 选项，并输入以分钟计的时间间隔。
   - 如果您想要创建更周密的计划，或者，创建针对每周中的各天的不同的计划，请选择 **设置和管理计划的更新** 选项，并单击 **添加**。

     在 **更新计划** 对话框中，输入计划名称，选择一周中的某一天，并输入更新频率。

17.9 配置更新管理器日志记录

如果您使用基于角色的管理，您必须具有 **策略设置 - 更新** 权限，才能配置更新管理器。 要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 如果您在 **终结点** 视图中，单击工具栏上的 **更新管理器** 按钮，以显示 **更新管理器** 视图。

2. 在更新管理器列表中，选择您想要为其配置日志文件的更新管理器。 单击鼠标右键，并单击 **查看/编辑配置**。
3. 在 **配置更新管理器** 对话框的 **日志记录** 标签页中，选择您想要保持日志记录的天数，以及日志文件的最大容量。

17.10 配置更新管理器更新自身

如果您使用基于角色的管理，您必须具有 **策略设置 - 更新** 权限，才能配置更新管理器。 要了解更多信息，请参见 关于角色和子领域 （第11页）。

1. 如果您在 **终结点** 视图中，单击工具栏上的 **更新管理器** 按钮，以显示 **更新管理器** 视图。
2. 在更新管理器列表中，选择您想要配置更新自身的更新管理器。 单击鼠标右键，并单击 **查看/编辑配置**。
3. 在 **配置更新管理器** 对话框的 **高级** 标签页中，选择您想要保持及时更新的更新管理器的版本。
   例如，如果您选择“建议”，那么，更新管理器将总是升级到 Sophos 提供的具有此标签的版本。 实际的更新管理器版本将改变。

17.11 使更新管理器立即检查更新文件

如果您使用基于角色的管理，您必须具备 **调整 - 更新和扫描** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域 （第11页）。

在您配置了更新管理器之后，它会按照设定的计划，检查更新文件，并自动将它们从更新源下载到它所维护的更新共享文件夹中。 如果您想要某个更新管理器，立即检查并下载安全隐患检测数据更新文件，终结点计算机的软件更新文件，以及更新管理器自身的软件更新文件，请按照以下步骤做:

1. 如果您在 **终结点** 视图中，单击工具栏上的 **更新管理器** 按钮，以显示 **更新管理器** 视图。
2. 在更新管理器列表中，选择您想要更新的更新管理器。 单击鼠标右键，并单击 **立即更新**。

17.12 监控更新管理器

1. 如果您在 **终结点** 视图中，单击工具栏上的 **更新管理器** 按钮，以显示 **更新管理器** 视图。
2. 在更新管理器列表中，查看 **警报** 和 **错误** 栏发现任何可能存在的问题。

3. 如果在某个更新管理器旁出现警报或错误图标，请单击该更新管理器，并单击 **查看更新管理器详情**。

   在 **计算机详情** 对话框中，您可以看到前次安全隐患检测数据和软件更新的时间，软件预订或更新管理器保持及时更新的软件预订的状态，以及更新管理器的状态。

4. 要了解更多有关某个特定的更新管理器的状态，以及有关怎样处置它的信息，请参见 **描述** 栏中的链接。

注: 如果更新管理器暂时不能更新，更新管理器的指标面板将不会报告错误或发出警报。只有当更新管理器最近一次更新的时间，超过了在创建或编辑更新计划（第72页）中所设定的警告级或紧要级的标准时，才会生成错误和警报。

17.13 使更新管理器遵照配置设置

如果您使用基于角色的管理，您必须具备 **调整-更新和扫描** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 如果您在 **终结点** 视图中，单击工具栏上的 **更新管理器** 按钮，以显示 **更新管理器** 视图。
2. 在更新管理器列表中，选择您想要遵照配置设置的更新管理器。 单击鼠标右键，并单击 **遵照配置**。

17.14 添加附加的更新管理器

Sophos Update Manager (SUM) 总是安装在您安装 Enterprise Console 的计算机上。 如果您在安装期间，选择了 **自定义安装**，那么，SUM 所安装的计算机，是安装了 Management Server 的计算机。

您添加一个或多个附加的更新管理器到网络中。这样做您可以减轻已安装的更新管理器的负荷，并且可以更有效地分发更新文件。 您安装附加的更新管理器的计算机，不一定非要已经安装了其它的更新管理器。

重要: 不要删除安装在 Enterprise Console 所在的管理服务器上的更新管理器。 在此更新管理器被配置更新源之前，Enterprise Console 无法彻底保护网络。 这使 Enterprise Console 能够收到必要的更新文件（例如，终结点计算机应该运行的安全软件的版本的信息，新的和更新的数据控制所使用的 “内容控制列表” (CCL)，或者，新的受控设备和受控程序的列表）。

要使附加的更新管理器能够通过 HTTP 从 Sophos 或其它的更新管理器下载安全软件，请开启您想要安装附加的更新管理器的计算机上的端口 80。 要使更

新管理器能够通过 UNC 路径从其它的更新管理器下载安全软件，请开启该计算机上的端口 137，138，139，以及 445。

如果计算机运行的 Windows 操作系统版本中包括 Network Discovery 功能，而该功能是关闭的，那么，请开启该功能并重新启动计算机。

如果计算机运行的是 Windows Server 2008 操作系统，那么，请关闭“用户帐户控制” (UAC) 并重新启动计算机。 在安装完毕更新管理器，并预订 Sophos 更新文件之后，您可以重新开启 UAC。

如果计算机运行的是 Windows 2000 操作系统，那么，在安装之后需要重新启动计算机。

如果计算机在域中，请以域系统管理员的身份登录。

如果计算机在工作组中，请以本地系统管理员的身份登录。

更新管理器安装程序在安装了 Enterprise Console 的管理服务器上的共享文件夹 \\Servername\SUMInstallSet 中。 要查看更新管理器安装程序的路径，转到 **视图** 菜单，并单击 **Sophos Update Manager 安装程序路径**。

您可以使用 Windows Remote Desktop 安装 Sophos Update Manager。

要安装附加的更新管理器:

1. 运行 Sophos Update Manager 安装程序文件 **Setup.exe**。

   会出现一个安装向导。

2. 在该向导的 **欢迎** 页面中，单击 **下一步**。
3. **在 用户使用许可协议** 页面中，仔细阅读许可证协议，如果您同意所有的条款，请单击 我接受许可证协议中的条款。 单击 **下一步**。
4. 在 **目标文件夹** 页面中，接受默认设置，或者，单击 **更改** 并输入新的目标文件夹。 单击 **下一步**。
5. 在 **Sophos Update Manager 帐户** 页中，选择终结点计算机将要用来访问由更新管理器创建的默认的更新共享的帐户。（默认的更新路径是: \\<计算机名>\SophosUpdate，这里的“计算机名”是更新管理器安装所在的计算机。）此帐户必须具备对共享的读权限，但不必具有管理员权限。

   您可以选择默认用户 ，选择现有的用户，或创建新的用户。

   依照默认值，安装程序会创建对默认的更新共享具有读权限的 **SophosUpdateMgr** 帐户，该帐户没有交互登录权限。

   如果您稍后想要添加更多的更新共享，请选择一个现有帐户，或创建对这些共享具备读权限的新帐户。 否则，请确保 **SophosUpdateMgr** 帐户对这些共享具有对权限。

6. 在 **Sophos Update Manager 帐户详情** 页中，根据您在先前的页面中选择的选项，输入默认用户的密码，或新用户的详情，或选择现有的帐户。

   帐户的密码必须遵照您的密码策略。

7. 在 **准备安装程序** 页中，单击 **安装**。
8. 当安装完成时，单击 **完成**。

您安装 Sophos Update Manager 的那台计算机，应该出现在 Enterprise Console 的 **更新管理器** 视图中。 在 **查看** 菜单，单击 **更新管理器**。

要配置更新管理器，请选择它，单击鼠标右键，然后，单击 **查看/编辑配置**。

17.15 在网页服务器上发布安全软件

您可能想在网页服务器上发布 Sophos 安全软件，使计算机可以通过 HTTP 进行访问。 如果您想要安装 Sophos Anti-Virus for UNIX 版本 4，那么，您必须这样做，尽管您可以根据需要，直到您下载了 Sophos Anti-Virus for UNIX 版本 4 之后，才这样做。

要在网页服务器上发布安全软件:

1. 要查找放置已下载的安全软件的共享文件夹的路径（也称为“引导路径”）:

   a) 在 Enterprise Console 中的 **查看** 菜单中，单击 **引导路径**。

      在 **引导路径** 对话框的 **路径** 栏中，会显示针对各个操作系统的引导路径。

   b) 记录下该路径，但是不要包括最后的中央安装目录(CID) 文件夹。例如:
      \\服务器名称\SophosUpdate

2. 网页服务器上提供此引导路径（包括子文件夹）。
3. 指定用户名和密码，已防止在网页服务器上，对此文件夹进行未经授权的访问。

注: 在网页服务器的技术文档中，应当有怎样在网络中共享文件夹，以及怎样为其设置用户名和密码的说明。要了解更多有关怎样做的信息，请联系您的网页服务器厂商。

18 配置防病毒和 HIPS 策略

18.1 关于防病毒和 HIPS 策略

防病毒和HIPS策略使您能够检测和清除病毒，特洛伊木马，蠕虫，间谍软件，以及广告软件和其它可能不想安装的应用程序。通过它，您还可以扫描计算机中的可疑行为，可疑文件，以及 Rootkit。您可以为每组计算机进行不同的设置。

依照默认值，在用户试图访问带有已知的和未知的病毒，特洛伊木马，蠕虫，以及间谍软件的文件时，Sophos Endpoint Security and Control 可以自动检测到它们。它还可以分析正在系统中运行的程序的行为。

您还可以配置 Sophos Endpoint Security and Control 进行以下工作:

- 扫描可疑文件（第79页）
- 扫描广告软件和可能不想安装的应用程序（第83页）
- 在设定的时间扫描计算机（第92页）

您可以在一旦发现病毒或其它安全隐患时，就自动清除计算机。要这样做，请按照 设置自动清除（第55页） 中的说明，更改读写扫描的设置。

注: 如果您使用基于角色的管理，那么，

- 您必须具有 **策略设置 - 防病毒和 HIPS** 的权限，以编辑防病毒和 HIPS 策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多有关基于角色的管理的信息，请参见关于角色和子领域（第11页）。

注: Enterprise Console 4.5 无法在 UNIX 计算机上执行读写扫描，也无法在 Mac 计算机上进行计划扫描。使用其它的扫描选项，或参见 *Sophos Anti-Virus for UNIX user manual*（英文） 或 *Sophos Anti-Virus for Mac OS X configuration guide*（英文） 了解更多的扫描选项。

18.2 扫描病毒，特洛伊木马，蠕虫，以及间谍软件

依照默认值，在用户试图访问带有已知的和未知的病毒，特洛伊木马，蠕虫，以及间谍软件的文件时，Sophos Endpoint Security and Control 可以自动检测到它们。

18.3 可疑行为和文件检测 (HIPS)

18.3.1 什么是 HIPS？

主机入侵防护系统 *(HIPS)* 是保护计算机免遭可疑文件，未识别病毒，以及可疑行为入侵的计算机安全技术。有两种 HIPS 方法：可疑行为检测，以及可疑文件检测。

注：HIPS 选项只应用于 Sophos Endpoint Security and Control for Windows 2000 及以后。

可疑行为检测

可疑行为检测，是对所有运行在计算机上的程序进行动态分析，以检测并阻断可能带有恶意的程序活动。可疑行为，如：使计算机在重新启动时，可能会允许病毒自动运行的注册表更改。

可疑行为检测包括“缓冲区溢出检测”，它可以动态地分析运行在系统中的所有程序的行为，以便检测缓冲区溢出攻击。

注：“缓冲区溢出检测”功能不能用于 Windows Vista，Windows 2008，Windows 7，以及 64 位版的 Windows。这些操作系统通过 Microsoft 的 Data Execution Prevention (DEP) 功能，来防范缓冲区溢出攻击。

要了解有关配置可疑行为检测的信息，请参见检测和阻断可疑行为（第78页）。

可疑文件检测

Sophos Endpoint Security and Control 可以扫描可疑文件。可疑文件中包含某些恶意软件所共有的特征，但是这些特征还不足以确定这些文件为新出现的恶意软件。

要了解有关配置可疑文件检测的信息，请参见扫描可疑文件（第79页）。

18.3.2 检测和阻断可疑行为

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见关于角色和子领域（第11页）。

依照默认值，Sophos Endpoint Security and Control 将分析在操作系统中运行的程序的行为，但是不会阻断显示可疑行为的程序。

Sophos 建议您在此“仅限警报”模式下，运行一次 Sophos Endpoint Security and Control，并批准您需要的程序之后，再启用自动阻断可疑行为。当检测到可疑行为或缓冲区溢出时，您可以删除或批准可疑项目。请参见 立即清除计算机（第54页） 和 批准可疑项目（第80页）。在批准了您需要的所有程序后，请启用阻断可疑行为。

1. 检查哪个防病毒和HIPS策略被您想要配置的一个或多个计算机组所采用了。请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的策略。
3. 在 **防病毒和 HIPS 策略** 对话框中，单击 **可疑行为 (HIPS)** 按钮。

   会出现 **可疑行为检测** 对话框。依照默认值，所有三个选项（**检测可疑行为**，**检测缓冲区溢出**，以及 **仅限警报**）都已启用。
4. 取消勾选 **仅限警报** 勾选框。

18.3.3 扫描可疑文件

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

可疑文件是指具有某些恶意软件共有的特征，但是又不足以确定为新出现恶意软件的文件（例如：含有恶意软件通常会使用的动态解压缩代码的文件）。

注: 此选项只应用于 Sophos Endpoint Security and Control for Windows 2000 及以后。

1. 检查哪个防病毒和HIPS策略被您想要配置的一个或多个计算机组所采用了。请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的策略。

3. 在 **防病毒和 HIPS 策略** 对话框中，按照以下说明设置选项:

   - **读写扫描**

     要配置读写扫描，在 **配置防病毒和 HIPS** 面板中，确保勾选了 **启用读写扫描** 勾选框。单击勾选框旁的 **配置** 按钮。

     在 **扫描** 标签页的 **扫描选项** 面板中，勾选 **扫描可疑文件 (HIPS)** 勾选框。单击 **确定**。

   - **计划扫描**

     要配置计划扫描，在 **计划扫描** 面板中，单击 **添加** （或者，选择某个现有的扫描，单击 **编辑** ）。

     在 **计划扫描设置** 对话框中，输入您的设置，然后，单击 **配置**。

     在 **扫描和清除设置** 对话框中的 **扫描** 标签页中，在 **扫描选项** 面板中，勾选 **扫描可疑文件 (HIPS)** 勾选框。单击 **确定**。

当检测到可疑文件时，您可以删除 或 批准 该文件。请参见 立即清除计算机（第54页）和 批准可疑项目（第80页）。

18.3.4 批准可疑项目

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

如果您启用了一个或多个 HIPS 选项（如: 可疑行为检测，缓冲区溢出检测，或可疑文件检测），但是，您想使用某些检测到的项目，您可以按照以下说明批准它们:

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。 然后，双击您想要更改的策略。
3. 在 **防病毒和 HIPS 策略** 对话框中，单击 **批准** 按钮。

4. 在 **批准管理器** 对话框中，单击已检测到的行为的类型的标签页，如：“缓冲区溢出”。
   - 要批准检测到的程序，请在 **已知的应用程序** 列表中找到该应用程序，并将它从 **已知的应用程序** 列表中移动到 **已批准的应用程序** 列表中。
   - 要允许 Sophos Endpoint Security and Control 尚未归类为可疑的项目，请单击 **新项目**。 浏览到该项目，选择并将它添加到 **已批准** 列表中。

如果您想从该列表中删除某个项目，请选择该项目，并单击 **删除项目**。 如果您已经批准了该项目，从该列表中删除该项目，将再次阻断该项目；所以，请只有在确信不再需要批准该项目的情况下，才使用这一选项。该选项不会将项目从磁盘中删除。

18.4 Sophos Live Protection

18.4.1 关于 Sophos Live Protection

Sophos Live Protection 使用云计算技术，不断地判断可疑文件是否成为安全隐患，并随时采取在“防病毒和 HIPS”策略中所指定的措施。

Sophos Live Protection 可以显著提高对新出现的恶意软件的检出率，同时也不会做无谓的检测活动。能够做到这一点，是因为能够随时比对最新的已知的恶意软件。一旦确认了新的恶意软件，Sophos 即可立即发出更新文件。

要充分利用 Sophos Live Protection 的优势，您必须确保启用了以下选项。

- **启用 Live Protection**

  如果终结点计算机上的防病毒扫描发现某个文件可疑，但是又无法根据存储在计算机上的安全隐患识别文件 (IDE) 进一步确认该文件中是否有恶意代码，那么，会将文件的某些特征，如：文件的检查和，发送给 Sophos 以便做进一步的分析。云计算检查会在SophosLabs数据库中迅速查看可疑文件。如果文件被确认为是正常的，或者是带有恶意代码的，确认意见会被寄给该计算机，并且该文件的状态会被自动更新。

- **自动发送文件样本给 Sophos**

  如果某个文件肯定会有恶意行为，但是却又不能仅仅根据其特征就肯定地确认它具有恶意代码，那么，Sophos Live Protection 会响应 Sophos 对此文件的样本的请求。如果此选项已启用，并且 Sophos 尚未具有该文件的样本，那么，该文件会被自动提交。

  提交类似的文件样本，有助于 Sophos 不断增强检测恶意软件的能力，并且降低误报的几率。

注: 样本的最大容量为 10 MB。样本上传的超时时限为 30 秒。不建议通过低速连接（低于 56 Kbps）自动发送样本。

重要: 您必须确保在网页过滤方案中将 Sophos 的域名设置为“信任的”，文件数据将会被寄往该域名。要了解详情，请参见技术支持知识库文章 62637 (*http://cn.sophos.com/support/knowledgebase/article/62637.html*)。

如果您使用的是 Sophos 的网页过滤方案，例如，WS1000 Web Appliance，那么，您不必进行任何操作 — Sophos 的域名已经是受信任的域名。

18.4.2 开启或关闭 Sophos Live Protection

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域 （第11页）。

依照默认值，Endpoint Security and Control 会向 Sophos 发送文件数据，如：检查和。但是，不会发送文件样本。要充分利用 Sophos Live Protection 的优势，您必须同时启用 Sophos Live Protection 的两个选项。

要开启或关闭 Live Protection 选项:

1. 检查哪个防病毒和HIPS策略被您想要配置的一个或多个计算机组所采用了。
   请参见 查看组采用的策略 （第24页）。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的策略。
3. 在 **防病毒和 HIPS 策略** 对话框中，单击 **Sophos Live Protection** 按钮。
4. 在 **Sophos Live Protection** 对话框中:
   - 要开启或关闭向 Sophos 发送文件数据，请勾选或取消勾选 **启用 Live Protection** 勾选框。
   - 要开启或关闭向 Sophos 发送文件样本，请勾选或取消勾选 **自动发送文件样本给 Sophos** 勾选框。

   注: 当向 Sophos 寄送文件样本进行在线扫描时，总是将文件数据同样本一同寄送。

18.5 扫描广告软件和可能不想安装的应用程序

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

注: 此选项只应用于 Sophos Endpoint Security and Control for Windows 2000 及以后。

Sophos建议您在开始时，使用计划扫描检测可能不想安装的应用程序。这使您可以安全地处理已经运行在您的网络中的可能不想安装的应用程序。此后，您可以再启用读写扫描来检测和保护您的计算机。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的策略。

   会出现 **防病毒和 HIPS 策略** 对话框。
3. 在 **计划扫描** 面板中，单击 **添加** 以创建一个新扫描，或者，双击列表中的某个扫描以编辑它。
4. 在 **计划扫描设置** 对话框中，单击 **配置** （在页面的底部）。
5. 在 **扫描和清除设置** 对话框中的 **扫描** 标签里，在 **扫描选项** 选项下，选择 **扫描广告软件和可能不想安装的应用程序**。单击 **确定**。

   在执行该扫描时，Sophos Endpoint Security and Control 可能会报告发现一些“广告软件和其它可能不想安装的应用程序”。
6. 如果您想允许在您的计算机上运行这些应用程序，您必须批准它们（参见 批准广告软件和可能不想安装的应用程序（第84页））。否则，请删除它们（参见 立即清除计算机（第54页））。
7. 如果您想要启用读写扫描，请再次打开 **防病毒和 HIPS 策略** 对话框。在 **配置防病毒和 HIPS** 面板中，确保勾选了 **启用读写扫描** 勾选框。单击勾选框旁的 **配置** 按钮。在 **读写扫描设置** 对话框中，选择 **扫描广告软件和可能不想安装的应用程序**。

   注: 有一些“监控”文件的应用程序，会试图频繁地访问文件。如果您启用了读写扫描，则读写扫描会检测到每一次读写，并发出多重警报。请参见 频繁发出有关可能不想安装的应用程序的警报（第178页）。

18.6 批准广告软件和可能不想安装的应用程序

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

如果您已启用了 Sophos Endpoint Security and Control 检测广告软件和其它可能不想安装的应用程序(PUA)，它可能阻止您想要使用的应用程序。

要批准这样的应用程序：

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的策略。
3. 在 **防病毒和 HIPS 策略** 对话框中，单击 **批准** 按钮。
4. 在 **批准管理器** 对话框中的 **广告软件和可能不想安装的应用程序** 标签里，在 **已知的广告软件和可能不想安装的应用程序** 列表，选择您想要的应用程序。单击 **添加** 将其添加到 **已批准的广告软件和可能不想安装的应用程序** 列表中。
5. 如果您无法看见您想要批准的应用程序，请单击 **新项目**。

   会出现 **添加新的广告软件 / 可能不想安装的应用程序** 对话框。
6. 转到 Sophos 安全分析网页，*http://cn.sophos.com/security/analyses* 中。在 **广告软件和可能不想安装的应用程序** 标签中，找到您想要批准的应用程序。
7. 在 Enterprise Console 的 **添加新的广告软件或可能不想安装的应用程序** 对话框中，输入您想要批准的应用程序的名称，并单击 **确定**。

   该程序已被添加到 **已知的广告软件和可能不想安装的应用程序** 列表中。
8. 选择该应用程序，并单击 **添加** 将其添加到 **已批准的广告软件和可能不想安装的应用程序** 列表中。

如果您想从该列表中删除某个应用程序，请选择该应用程序，并单击 **删除项目**。

18.7 更改要扫描的文件类型

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

依照默认值，Sophos Endpoint Security and Control 会对各种容易被病毒感染的文件类型进行扫描。您可以扫描附加的文件类型，或者，选择从扫描中排除某些文件类型。

默认扫描的文件类型，在不同的操作系统上会有所不同，并且在软件更新后，可能发生改变。要查看文件类型，请在相应的操作系统的计算机上，打开 Sophos Endpoint Security and Control 窗口，找到"排除项目"配置页面。

注:

这些选项仅仅应用于 Windows 计算机。

在 Windows 2000 或以后的操作系统中，您可以分别为读写扫描和计划扫描更改设置。在 Windows NT/95/98 操作系统中，在计划扫描中所作的更改，会同时被应用于读写扫描。

您可以使用 Sophos Update Manager 在 Mac OS X 计算机上更改防病毒设置，Sophos Update Manager 是随 Sophos Anti-Virus for Mac OS X 提供的一个工具软件。要打开 Sophos Update Manager，请在 Mac OS X 计算机的 **Finder** 窗口中，浏览找到 Sophos Anti-Virus:ESOSX 文件夹。双击 **Sophos Update Manager**。要了解更多详情，请参见 Sophos Update Manager 帮助文件。

您可以按照 Sophos Anti-Virus for Linux 用户手册中的说明，使用 savconfig 和 savscan 命令，更改 Linux 计算机上的设置。

您可以按照 Sophos Anti-Virus for UNIX 用户手册中的说明，使用 savscan 命令，更改 UNIX 计算机上的设置。

要更改要扫描的文件类型:

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。
   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的策略。

3. 在 **防病毒和 HIPS 策略** 对话框中，按照以下说明设置选项:
   - 要配置读写扫描，在 **配置防病毒和 HIPS** 面板中，确保勾选了 **启用读写扫描** 勾选框。单击勾选框旁的 **配置** 按钮。
   - 要配置计划扫描，请在 **计划扫描** 栏中，单击 **扩展名和排除文件**。
4. 在 **扩展名** 标签页中，选择 **扫描可执行和可感染文件**。
   - 要扫描附加的文件类型，请单击 **添加**，然后，在 **扩展名** 栏中，键入文件类型的扩展名，如: PDF。
   - 要免去扫描某些，通常默认扫描的文件类型，请单击 **排除文件**。这会打开 **排除文件扩展名** 对话框。输入文件扩展名。

   依照默认值，会扫描没有扩展名的文件。

   注: 您还可以选择扫描所有文件，尽管这会影响计算机的运行效率。

18.8 从读写扫描中排除项目

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以排除要进行读写扫描的项目。

注:

这些选项只应用于 Windows 2000 或以后，Mac OS X，以及 Linux。

Enterprise Console 4.5 无法在 UNIX 计算机上执行读写扫描。

要在 Windows NT/95/98 计算机上排除项目，请使用计划扫描配置页，在该页面中的配置同样可以应用于读写扫描。请参见 从计划扫描中排除项目（第93页）。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的策略。

   会出现 **防病毒和 HIPS 策略** 对话框。
3. 在 **读写扫描** 面板中，单击 **配置** 按钮。

4. 单击 **Windows 排除项目**，**Mac 排除项目**，或 **Linux/UNIX 排除项目** 标签页。要添加项目到列表中，请单击 **添加**，然后，在 **排除项目** 对话框中输入完整的路径。

   您可以从扫描中排除的项目，因计算机的类型会有所不同。请参见 可以从扫描中排除的项目（第94页）。

18.9 扫描 rootkit

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

当您在计算机上运行 完整系统扫描 时，扫描 rootkit 总是会执行（参见 现在扫描计算机（第62页））。但是，如果您想要更改计划扫描的设置，请按照以下说明做。

注: 此选项只应用于 Sophos Endpoint Security and Control for Windows 2000 及以后。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。 然后，双击您想要更改的策略。
3. 在 **防病毒和 HIPS 策略** 对话框的 **计划扫描** 面板中，单击 **添加**（或者选择现有的扫描，并单击 **编辑**）。
4. 在 **计划扫描设置** 对话框中，输入您的设置，然后，单击 **配置**。
5. 在 **扫描和清除设置** 对话框中的 **扫描** 标签页中，勾选 **启用 Rootkit 扫描** 勾选框。单击 **确定**。

18.10 扫描打包文件内部

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

注: 扫描打包文件内部会显著减慢扫描进程，通常并不需要使用。 即使您没有选择该选项，当您试图访问从打包文件中解包的文件时，该解包文件也会被扫描。 Sophos 因此不推荐使用这一选项。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。

2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。 然后，双击您想要更改的策略。
3. 在 **防病毒和 HIPS 策略** 对话框的 **计划扫描** 面板中，单击 **添加**（或者选择现有的扫描，并单击 **编辑**）。
4. 在 **计划扫描设置** 对话框中，输入您的设置，然后，单击 **配置**（在该页的底部）。
5. 在 **扫描和清除设置** 对话框中的 **扫描** 标签页里，选择 **扫描打包文件内部**。 单击 **确定**。

18.11 扫描 Macintosh 文件

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以启用 Sophos Endpoint Security and Control 扫描存储在 Windows 计算机上的 Macintosh 文件。

注: 此选项只应用于 Sophos Endpoint Security and Control for Windows 2000 及以后。

1. 检查哪个防病毒和HIPS策略被您想要配置的一个或多个计算机组所采用了。

   请参见 查看组采用的策略（第24页）。

2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的策略。

3. 在 **防病毒和 HIPS 策略** 对话框中，按照以下说明设置选项:

   - **读写扫描**

     要配置读写扫描，请在 **读写扫描** 面板中，确保勾选了 **启用读写扫描** 勾选框。单击勾选框旁的 **配置** 按钮。

     在 **扫描** 标签页的 **扫描选项** 面板中，勾选 **扫描 Macintosh 病毒** 勾选框。
   - **计划扫描**

     要配置计划扫描，在 **计划扫描** 面板中，单击 **添加**（或者，选择某个现有的扫描，单击 **编辑**）。

     在 **计划扫描设置** 对话框中，输入您的设置，然后，单击 **配置**。

     在 **扫描和清除设置** 对话框中的 **扫描** 标签页中，勾选 **扫描 Macintosh 病毒** 勾选框。

18.12 关于网页防范

通过防止访问已知的带有恶意软件的网站，网页防范功能，可以提供增强的防范网页安全隐患的保护措施。通过实时对比 Sophos 的在线恶意网站数据库，它会阻断终结点计算机访问恶意网站。

网页防范会:

- 阻断网络访问恶意网站。
- 扫描通过 IE 浏览器下载的数据和文件。

要了解有关怎样启用网页扫描的信息，请参见 启用网页防范（第89页）。

18.13 启用网页防范

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

要启用网页防范:

1. 检查哪个防病毒和HIPS策略被您想要配置的一个或多个计算机组所采用了。请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的策略。

3. 在 **防病毒和 HIPS** 策略对话框中，请在 **阻断访问恶意网站** 旁，勾选 **开启**。依照默认值，此选项是启用的。

   要了解有关怎样批准特定的网站的信息，请参见 批准网站（第90页）。

4. 要扫描通过 IE 浏览器下载的数据和文件，请在 **下载扫描** 旁，勾选 **开启**。

   如果您想同时禁用或启用读写扫描和下载扫描，您还可以勾选 **在读写访问时**。

18.14 批准网站

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。



小心: 请在批准网站之前，确保访问该网站是安全的。批准已被归类为恶意网站的网站，会使您处于安全隐患之中。

如果您不想阻断已被 Sophos 归类为恶意网站的某个网站，那么，您可以将它添加到已批准的网站的列表中。批准某个网站，将会使该网站的 URL 避免 Sophos 扫描网站过滤服务的验证。

注: 如果您启用了扫描下载内容，并且使用 IE 浏览器访问某个含有安全隐患的网站，那么，即使该网站已列示在已批准的网站列表中，对它的访问仍然会被阻断。

要批准网站:

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。

2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的策略。
3. 在 **防病毒和 HIPS 策略** 对话框中，单击 **批准** 按钮。
4. 在 **批准管理器** 对话框的 **网站** 标签页中，单击 **添加**，通过所提供的选项之一，添加网站。

   您可以通过输入域名，IP 地址，或带有子网掩码的 IP 地址。

如果您想编辑或删除列表中的网站，请勾选网站，并相应地单击 **编辑** 或 **删除**。

要最近在某个终结点计算机上被阻断的网站的名单，请参见 查看被阻断的网站（第61页）。

18.15 开启或关闭读写扫描

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

依照默认值，Sophos Endpoint Security and Control 会在用户读写文件时扫描该文件，如果发现该文件感染了病毒，则会拒绝用户访问该文件。

您出于提高运行效率的考虑，可能会决定在Exchange服务器或其它服务器上，关闭读写扫描。在这种情况下，请将这些服务器放到一个专门的组中，并按照下面的说明更改组的防病毒和 HIPS 策略。

重要: 如果您关闭了服务器上的读写扫描，建议您在与该服务器相关的工作站上设置计划扫描。

1. 检查哪个防病毒和HIPS策略被您想要配置的一个或多个计算机组所采用了。

   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的策略。

   会出现 **防病毒和 HIPS 策略** 对话框。
3. 要关闭读写扫描，请取消勾选 **启用读写扫描** 勾选框。然后，在 **计划扫描** 面板中，单击 **添加** 并设置计划扫描。

如果您以后想重新启用读写扫描，请再次勾选 **启用读写扫描** 勾选框。

18.16 更改实行读写扫描的时机

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以指定，当您打开文件（“读文件时”），保存文件（“写文件时”），或者，文件重命名时，是否扫描文件。

注:

在“写文件时”或“重命名文件时”进行扫描，会对计算机的运行效率产生影响。这些选项一般不建议使用。

这些选项仅仅应用于 Windows 计算机。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。

2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的策略。
3. 在 **防病毒和 HIPS 策略** 对话框的 **读写扫描** 面板中，单击 **配置** 按钮。
4. 在 **读写扫描设置** 对话框中的 **扫描** 标签页中，在 **读写扫描行为** 面板中，选择您想要的选项。

18.17 在设定的时间扫描计算机

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以在设定的时间扫描计算机。

注: 计划扫描只在 Windows，UNIX 和 Linux 操作系统计算机上运行。 在 Windows 95/98 计算机中，计划扫描只在 Sophos Anti-Virus 窗口打开时，才会运行。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。

2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。 然后，双击您想要更改的策略。
3. 在 **防病毒和 HIPS 策略** 对话框的 **计划扫描** 面板中，单击 **添加**。
4. 在 **计划扫描设置** 对话框中，为扫描任务输入名称。 选择要扫描的项目（依照默认值，会扫描所有的本地硬盘或挂上(mounted)的文件系统）。 选择您想运行该扫描的日期和时间。
5. 如果您更改其它扫描选项，或配置该扫描清除计算机，请单击在该对话框底部的 **配置**。

   要了解关于怎样更改计划扫描的选项的信息，请参见 更改计划扫描设置（第92页）。

18.18 更改计划扫描设置

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。

■ 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

要更改已计划的扫描的设置:

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。
   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。 然后，双击您想要更改的策略。
3. 在 **防病毒和 HIPS 策略** 对话框的 **计划扫描** 面板中，更改需要更改的设置。
   您可以更改两种不同的设置:
   ■ 要更改所有的计划扫描都扫描的文件类型，单击 **扩展名和排除文件名**。
   ■ 要更改针对每一个扫描的具体设置（扫描项目，时间，扫描选项，清除），高亮选择该扫描，并单击 **编辑**。 然后，在 **计划扫描设置** 对话框中，单击 **配置**。

   注: 要了解怎样使用扫描选项的所有详情，请参见扫描可疑文件（第79页），扫描广告软件和可能不想安装的应用程序（第83页），和 扫描打包文件内部（第87页）。 要了解怎样使用清除选项的详情，请参见 设置自动清除（第55页）。

18.19 从计划扫描中排除项目

如果您使用基于角色的管理，那么，

■ 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。

■ 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以排除要进行计划扫描的项目。

注:

计划扫描中的“排除项目”设置，同样应用于从控制台运行的完整系统扫描，以及应用于在联网计算机上运行的“扫描我的电脑”。 请参见 现在扫描计算机（第62页）。

在 Windows NT/95/98 操作系统中，在计划扫描中所作的更改，会同时被应用于读写扫描。

在 Mac 计算机上不支持计划扫描。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。 然后，双击您想要更改的策略。
3. 会出现 **防病毒和 HIPS 策略** 对话框。 在 **计划扫描** 面板中，单击 **扩展名和排除文件**。
4. 单击 **Windows 排除文件** 或 **Linux/UNIX 排除文件** 标签页。 要添加项目到列表中，请单击 **添加**，然后，在 **排除项目** 对话框中输入完整的路径。

   您可以从扫描中排除的项目，因计算机的类型会有所不同。 请参见 可以从扫描中排除的项目（第94页）。

18.20 可以从扫描中排除的项目

在每种不同的操作系统的计算机上，对所能够从扫描中排除的项目，会有不同的限制。

Windows 2000 和以后

在 Windows 2000 或以上的计算机中，您可以排除驱动器，文件夹和文件。

您可以使用通配符 * 和 ?

通配符 ? 只能用于文件名或文件扩展名中。 一般地，它可以匹配任何单一的字符。 然而，在文件名或扩展名的最后使用通配符时，它匹配单个字符，或者，不匹配字符。 例如： file??.txt 可以匹配 file.txt，file1.txt 和 file12.txt， 但是不匹配 file123.txt。

通配符 * 仅能以 [filename].* 或 *.[extension] 的形式用于文件名或扩展名中。 比如，file*.txt，file.txt* 及 file.*txt 是无效的。

要了解更多详情，请参见供终结点计算机使用的软件 Sophos Endpoint Security and Control 版本 9 的帮助文件中的“使用 Sophos Anti-Virus” 部分。

Windows NT

在 Windows NT 计算机中，您可以排除文件和目录。

Windows 95/98

在 Windows 95/98 计算机中，您可以排除文件，目录（针对计划扫描），以及驱动器。

Mac OS X

在 Mac OS X 中，您可以排除卷，文件夹，以及文件。

尽管不支持使用通配符，您还是可以通过在欲排除的项目的前面或后面添加斜线或双斜线，来将其排除。

要了解更多的详情，请参见 Mac OS X 的有关帮助文件或用户手册。

Linux 或 UNIX

在 Linux 和 UNIX 中，您可以通过指定路径（带有或不带有通配符）来排除目录和文件。

注: Enterprise Console 只支持基于路径的 Linux 和 UNIX 排除项目。 您还可以在已管理的计算机上，直接设置其它类型的排除项目。 然后，您可以使用通常表示方式，排除文件类型和文件系统。 要了解操作指导，请参见 *Sophos Anti-Virus for Linux* 用户手册（英文），或 *Sophos Anti-Virus for UNIX* 用户手册（英文）。

如果您在已管理的Linux或UNIX计算机上，设置另一个基于路径的排除项目，该计算机将被作为具有不一致的组策略的计算机，报告给控制台。

19 配置更新策略

19.1 关于更新策略

更新策略使您能够保持您的计算机及时更新您所选择的安全软件。 Enterprise Console 将按照设定的频率检查更新文件，并在需要时，更新计算机。

默认的更新策略使您能够安装和更新在“最新”软件预订中指定的软件。

如果您想要更改默认的更新策略，或者，想要创建新的更新策略，请按照以下主题中的操作指导做:

- 选择预订（第96页）
- 选择更新源（第96页）
- 计划更新（第97页）
- 选择不同的初始安装源（第98页）
- 日志记录更新活动（第99页）

如果您是从 Enterprise Console 3.x 中升级的，在升级之前存在的更新策略会变成“继承性更新策略”。要了解更多有关继承性更新的信息，请参见“继承性更新”部分。

注: 如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 更新** 权限，才能配置更新策略。

- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多有关基于角色的管理的信息，请参见关于角色和子领域（第11页）。

19.2 选择预订

如果您使用基于角色的管理，那么，：

- 您必须具备 **策略设置 - 更新** 权限，才能配置更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

预订指定从 Sophos 为各操作平台的计算机下载哪个版本的终结点软件。 默认的预订包括针对 Windows 2000 及以后的最新软件。

要选择预订:

1. 检查哪个更新策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **更新**。 然后，双击您想要更改的策略。
3. 在 **更新策略** 对话框中，单击 **预订** 标签页，并选择您想要与之保持更新的软件的预订。

19.3 选择更新源

如果您使用基于角色的管理，那么，：

- 您必须具备 **策略设置 - 更新** 权限，才能配置更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

依照默认值，计算机从 UNC 共享：\\<ComputerName>\SophosUpdate 进行更新，这里的“计算机名”是更新管理器安装所在的计算机。 您可以指定不同的共享。

您还可以设置一个备用更新源。 如果计算机无法连接到常规的更新源，它会尝试从备用更新源进行更新。 如果您使用并不总是连接到网络中的计算机，例如：笔记型电脑，Sophos 建议您为更新文件设置备用更新源。

要指定更新源:

1. 检查哪个更新策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。

2. 在 **策略** 窗格板中，双击 **更新**。 然后，双击您想要更改的策略。
3. 在 **更新策略** 对话框中:
   - 如果您想要更改默认的主更新源，请转到 **主服务器** 标签页。
   - 如果您想要设置备用更新源，请转到 **副服务器** 标签页，并选择 **设定副服务器详情**。
4. 在 **更新策略** 对话框的 **主服务器** 标签页中的 **地址** 栏中，输入终结点计算机通常用来下载更新文件的共享的地址（UNC（网络）路径或网页地址）。

   重要: 如果您选择使用 HTTP 路径（例如，网页更新共享）或者，不是由更新管理器管理的共享文件夹，Enterprise Console 将不能够检查在预订策略中指定的软件是否从该地址可以获得。 您必须确保该共享文件夹中包含预订策略中所指定的软件。 否则，计算机将不会被更新。

5. 如果您想要使用从 Enterprise Console 管理的 Mac 计算机，并且您在 **地址** 栏的 **Mac OS 特定选项** 下，指定了 UNC 路径，那么，请选择 Mac 将用来访问更新共享的协议。
6. 如果必要，请在 **用户名** 栏中，输入将要用来访问服务器的帐户的用户名，然后，输入并确认密码。 该帐户应该拥有读取您在上面的地址栏中输入的共享的权限。

   注: 如果“用户名” 需要指明域，才算合格有效。请使用“域\用户名” 的形式。

7. 如果您想限制所使用的带宽，单击 **高级**。 在 **高级设置** 对话框中，选择 **限制带宽使用量**，并使用滑动控制条指定以“千字节/每秒”为单位的带宽量。如果您指定的带宽量超过了计算机所能提供的量，更新工作将使用计算机能提供的所有带宽。
8. 如果您是通过代理服务器接入更新源的，请单击 **代理详情**。 在 **代理详情** 对话框中，选择 **通过代理接入服务器**。 然后，输入代理服务器的 **地址** 和 **端口** 号。 输入用来接入代理服务器的 **用户名** 和 **密码**。 如果“用户名” 需要指明域，才算合格有效。请使用“域\用户名” 的形式。

   请注意，有的因特网服务提供商（ISP），要求将网页请求送到代理服务器上。

19.4 计划更新

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 更新** 权限，才能配置更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

依照默认值，计算机每隔 5 分钟做一次更新检查。

注: 如果计算机是直接从 Sophos 下载更新文件，则该更新频率设置不会被应用。 运行 Sophos PureMessage 的计算机会每隔15分钟检查一次更新文件。 没有运行 Sophos PureMessage 的计算机将每隔60分钟更新一次。

要指定更新频率:

1. 检查哪个更新策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。

2. 在 **策略** 窗格板中，双击 **更新**。 然后，双击您想要更改的策略。
3. 在 **更新策略** 对话框的 **计划** 标签页中，保留勾选 **启用联网计算机自动使用 Sophos 更新文件** 勾选框。 请输入软件更新的频率（以分钟计）。
4. 如果计算机是通过拨号连接因特网进行更新的，请选择 **在拨号连接时进行更新检查**。

   每当您连接到因特网时，计算机就会尝试进行更新。

19.5 选择不同的初始安装源

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 更新** 权限，才能配置更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

依照默认值，计算机软件安装在计算机上之后，就从在 **主服务器** 标签页中指定的更新源保持更新。 您可以指定不同的初始安装源

注:

这一设置仅仅应用于 Windows 2000 及以后的计算机上。

如果您的主服务器使用的是 HTTP 地址，而您想从控制台实施安装程序，那么，您必须在此指定初始安装源。

要从不同的安装源进行安装:

1. 检查哪个更新策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。

2. 在 **策略** 窗格板中，双击 **更新**。 然后，双击您想要更改的策略。

3. 在 **更新策略** 对话框的 **初始安装源** 标签种，取消勾选 **使用主服务器地址** 勾选框。 然后，输入您想使用的安装源的地址。

19.6 日志记录更新活动

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 更新** 权限，才能配置更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

依照默认值，计算机会日志记录它们的更新活动。默认的日志记录的最大容量为 1 MB。 默认的日志级别为“普通”。

要更改日志记录设置:

1. 检查哪个更新策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **更新**。 然后，双击您想要更改的策略。
3. 在 **更新策略** 对话框的 **日志记录** 标签页中，保留勾选 **记录 Sophos AutoUpdate 活动日志** 勾选框。 在 **日志文件大小上限** 栏中，指定日志文件的最大值。
4. 在 **日志记录级别** 栏中，选择 **普通** 或 **详尽** 日志记录。

   详尽的日志记录提供比通常的活动多得多的活动的信息，因而，日志文件的尺寸也会快速增大。 请只有在需要用它来处理出现的问题时，才使用这一设置。

19.7 更改主服务器的认证资料

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 更新** 权限，才能配置更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

要更改主服务器的认证资料:

1. 在 **策略** 窗格板中，双击 **更新**。 然后，双击您想要更改的那个更新策略。
2. 在 **更新策略** 对话框的 **主服务器** 标签页中，输入访问该服务器时所使用的新的认证资料。 如果需要，更改其它的详情。

3. 在 **组** 窗格板中，选择使用您刚更改的更新策略的某个组。右击鼠标，并选择 **遵照，组更新策略**。

   为使用此更新策略的各个组重复此步骤。

19.8 更新并不总是联网的计算机

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 更新** 权限，才能配置更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

对于并不总是联网的计算机，例如，笔记本电脑常常在办公室之外使用，您可以配置当它们在办公室之外时，从备用更新源进行更新。

备用更新源可以是您的公司维护的网站中的某个更新文件夹，也可以是Sophos网站。要了解有关怎样在网页服务器上创建更新文件夹的信息，请参见 在网页服务器上发布安全软件（第76页）。

要设置备用更新源:

1. 请检查您想要配置的计算机组使用的是哪个更新策略。请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **更新**。然后，双击您想要更改的策略。
3. 在 **更新策略** 对话框的 **副服务器** 标签页中，选择 **指定副服务器详情**。
4. 在 **地址** 文本框中，输入共享地址（UNC路径或网址），如果无法连接常用的更新源时，终结点计算机将从该共享下载更新文件。

   重要: 如果您选择使用 HTTP 路径（例如，网页更新共享）或者，不是由更新管理器管理的共享文件夹，Enterprise Console将不能够检查在预订策略中指定的软件是否从该地址可以获得。您必须确保该共享文件夹中包含预订策略中所指定的软件。否则，计算机将不会被更新。

5. 如果必要，请在 **用户名** 栏中，输入将要用来访问服务器的帐户的用户名，然后，输入并确认密码。

   该帐户应该：

   - 对您在上述的地址栏中输入的共享，具有读访问（能够浏览）的权限。
   - 能够登录到组中的计算机上。

   要了解更多有关怎样检查 Windows 用户帐户的信息，请参见 Sophos 技术支持知识库文章 11637 (*http://cn.sophos.com/support/knowledgebase/article/11637.html*)。

   注: 如果“用户名” 需要指明域，才算合格有效。请使用“域\用户名” 的形式。

6. 如果您想限制所使用的带宽，单击 **高级**。 在 **高级设置** 对话框中，选择 **限制带宽使用量**，并使用滑动控制条指定以“千字节/每秒”为单位的带宽量。如果您指定的带宽量超过了计算机所能提供的量，更新工作将使用计算机能提供的所有带宽。
7. 如果您是通过代理服务器接入更新源的，请单击 **代理详情**。 在 **代理详情** 对话框中，选择 **通过代理接入服务器**。 然后，输入代理服务器的 **地址** 和 **端口** 号。 输入用来接入代理服务器的 **用户名** 和 **密码**。 如果“用户名” 需要指明域，才算合格有效。请使用“域\用户名” 的形式。

   请注意，有的因特网服务提供商（ISP），要求将网页请求送到代理服务器上。

20 继承性更新

20.1 关于继承性更新

当您从 Enterprise Console 3.x 升级时，在升级之前存在的更新策略会变成“继承性更新策略”。 使用新的更高效的技术的 Sophos Update Manager，会被安装，并根据您先前（来自 Sophos EM Library）的更新设置被配置。 EM Library to Update Manager 迁移向导会帮助您迁移将要由更新管理器来更新的 Enterprise Console 计算机组。 任何不能被向导迁移的组，将继续使用继承性更新策略。

要了解怎样迁移尚未被该向导迁移的组的操作指导，请参见 *Sophos Endpoint Security and Control* 高级升级指南。

如果在迁移之前，您想继续有时使用继承性更新策略，请参见设置继承性更新（第102页），了解怎样设置或更改相关设置的操作指导。

要了解有关设置 EM Library 和创建中央安装目录 (CID) 的信心，请参见 EM Library Help（英文）。要开启 EM Library，请在指标面板的 **更新文件** 部分，单击 **EM Library 最新更新于 <时间>** 链接。

注: 如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 更新** 权限，才能配置继承性更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多有关基于角色的管理的信息，请参见关于角色和子领域（第11页）。

20.2 设置继承性更新

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 更新** 权限，才能配置继承性更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

您必须针对将要应用该更新策略的组中的各个类型的计算机（如: Windows 2000 及以后），按照以下步骤做。

要设置继承性更新:

1. 打开相应的继承性更新策略。
   - 要创建新的继承性更新策略，请在 **策略** 窗格板中，右击 **继承性更新**，然后，选择 **创建策略**。输入策略名称，然后按 **输入** 按钮保存该名称。双击新策略，可以编辑它。
   - 要编辑默认策略，双击 **继承性更新**，然后，双击 **默认值**。
   - 要编辑早先创建的策略，请检查哪个更新策略被您想要配置的计算机组所使用。（请参见查看组采用的策略（第24页）。）在 **策略** 窗格板中，双击 **继承性更新**。然后，双击您想要更改的策略。
2. 在 **继承性更新策略** 对话框中，选择一个操作系统。单击 **配置**。

3. 在 **设置更新策略** 对话框，单击 **主服务器** 标签，并设置以下说明的选项。

   地址

   输入 Sophos Anti-Virus 通常可以下载获取更新文件的地址（UNC （网络）路径或网站地址）。 要了解默认的更新目录 (CID) 列表，请参见 默认的继承性更新目录（第109页）。

   用户名

   如有必要，在 **用户名** 中输入将用来接入服务器的帐户名，然后，输入并确认 **密码**。 该帐户应该拥有读取您在上面的地址栏中输入的路径的权限。

   注: 如果 **用户名** 需要指明域，才算合格有效，请使用“域\用户名”的形式。

   高级和代理详情

   如果您想限制所使用的带宽，单击 **高级**。 请参见 限制带宽使用量（第107页）。

   如果您是通过代理服务器接入更新源的，请单击 **代理详情**。 请参见 指定用于继承性更新的代理服务器（第107页）。 请注意，有的因特网服务提供商（ISP），要求将网页请求送到代理服务器上。

4. 单击 **计划** 标签，然后按照以下说明输入详情。

   启用网络中的计算机自动使用 Sophos 更新文件

   如果您想要计算机定期更新，请选择此项。 然后，输入更新频率（以分钟为单位），计算机将按照此频率检查更新文件。 默认值是5分钟。

   注: 如果计算机是直接从Sophos下载更新文件，则该频率设置不会被应用。 运行 Sophos PureMessage 的计算机会每隔15分钟检查一次更新文件。 没有运行 Sophos PureMessage 的计算机将每隔60分钟更新一次。

   在拨号连接时作更新检查

   如果计算机是通过拨号连接到因特网进行更新工作的，请选择该项。 每当您连接到因特网时，计算机就会尝试进行更新。

5. 在 **策略** 窗格板中，单击新的策略，并将其拖放到您想要配置的计算机组中。

   注: 如果您只不过是编辑某个已经应用到组中的策略，如：默认的策略，那么，您不必进行步骤5。

20.3 为继承性更新选择更新源

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 更新** 权限，才能配置继承性更新策略。

- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域 (第11页) 。

如果您想要计算机能够自动更新，您必须为它们指定取得更新文件的地方。

注: 您必须指定，各个类型的计算机 (如: Windows 2000 及以后) 取得更新文件的地方。

1. 检查您想要配置的计算机组所采用了哪个继承性更新策略。
   请参见 查看组采用的策略 (第24页) 。
2. 在 **策略** 窗格板中，双击 **继承性更新**。然后，双击您想要更改的策略。
3. 在 **继承性更新策略** 对话框中，选择一个操作系统。单击 **配置**。
4. 在 **设置更新策略** 对话框，单击 **主服务器** 标签。请按以下说明设置选项。

   地址

   输入 Sophos Anti-Virus 通常可以下载获取更新文件的地址 (UNC (网络) 路径或网站地址) 。要了解默认的更新目录 (CID) 列表，请参见 默认的继承性更新目录 (第109页) 。

   用户名

   如有必要，在 **用户名** 中输入将用来接入服务器的帐户名，然后，输入并确认 **密码**。该帐户应该拥有读取您在上面的地址栏中输入的路径的权限。

   注: 如果 **用户名** 需要指明域，才算合格有效，请使用 “域\用户名” 的形式。

   高级和代理详情

   如果您想限制所使用的带宽，单击 **高级**。请参见 限制带宽使用量 (第107页) 。

   如果您是通过代理服务器接入更新源的，请单击 **代理详情**。请参见 指定用于继承性更新的代理服务器 (第107页) 。请注意，有的因特网服务提供商 (ISP) ，要求将网页请求送到代理服务器上。

20.4 为继承性更新选择备用更新源

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 更新** 权限，才能配置继承性更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域 (第11页) 。

您可以设置一个备用更新源。如果计算机无法连接到常规的更新源，它会尝试从备用更新源进行更新。

如果您使用并不总是连接到网络中的计算机，例如：笔记型电脑，Sophos建议您为更新文件设置备用更新源。

注: 您必须指定，各个类型的计算机（如：Windows 2000 及以后）取得更新文件的地方。

1. 检查您想要配置的计算机组所采用了哪个继承性更新策略。

   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **继承性更新**。然后，双击您想要更改的策略。
3. 在 **继承性更新策略** 对话框中，选择一个操作系统。单击 **配置**。
4. 在 **设置更新策略** 对话框，单击 **副服务器** 标签。选择 **指定副服务器详情**。然后，按照以下说明输入所需的详情。

   地址

   输入如果计算机无法连接到常规的更新源时，可以另外用来下载更新文件的 **地址**（UNC（网络）路径或网站地址）。如果您选择 Sophos，Sophos Anti-Virus 将通过因特网直接从 Sophos 下载更新文件。

   用户名

   如有必要，在 **用户名** 中输入将用来接入服务器的帐户名，然后，输入并确认 **密码**。该帐户应该拥有读取您在上面的地址栏中输入的路径的权限。

   注: 如果 **用户名** 需要指明域，才算合格有效，请使用“域\用户名”的形式。

   高级和代理详情

   如果您想限制所使用的带宽，单击 **高级**。请参见 限制带宽使用量（第107页）。

   如果您是通过代理服务器接入更新源的，请单击 **代理详情**。请参见 指定用于继承性更新的代理服务器（第107页）。请注意，有的因特网服务提供商（ISP），要求将网页请求送到代理服务器上。

20.5 计划继承性更新

如果您使用基于角色的管理，那么，：

- 您必须具备 **策略设置 - 更新** 权限，才能配置继承性更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以设定使用继承性更新的计算机进行更新的时间和频率。

注: 您要针对各个类型的计算机（如: Windows 2000 及以后），分别输入这些设置。

1. 检查您想要配置的计算机组所采用了哪个继承性更新策略。

   请参见 查看组采用的策略（第24页）。

2. 在 **策略** 窗格板中，双击 **继承性更新**。 然后，双击您想要更改的策略。
3. 在 **继承性更新策略** 对话框中，选择一个操作系统。 单击 **配置**。
4. 在 **设置更新策略** 对话框，单击 **计划** 标签。 按照以下说明输入所需的详情。

   启用网络中的计算机自动使用 Sophos 更新文件

   如果您想要计算机定期更新，请选择此项。 然后，输入更新频率（以分钟为单位），计算机将按照此频率检查更新文件。 默认值是5分钟。

   注: 如果计算机是直接从Sophos下载更新文件，则该频率设置不会被应用。运行 Sophos PureMessage 的计算机会每隔15分钟检查一次更新文件。 没有运行 Sophos PureMessage 的计算机将每隔60分钟更新一次。

   在拨号连接时作更新检查

   如果计算机是通过拨号连接到因特网进行更新工作的，请选择该项。 每当您连接到因特网时，计算机就会尝试进行更新。

20.6 现在更新计算机

如果您使用基于角色的管理，您必须具备 **调整 - 更新和扫描** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以立即更新一个或数个计算机，无需等到下一次自动更新。

1. 选择您要更新的计算机。
2. 右击并选择 **立即更新计算机**。

20.7 使计算机在拨号连接时更新

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 更新** 权限，才能配置继承性更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

如果您想要计算机，只要一拨号连接，就使用继承性更新进行更新，请按以下说明做:

注: 您要针对各个类型的计算机（如: Windows 2000 及以后），分别输入这些设置。

1. 检查您想要配置的计算机组所采用了哪个继承性更新策略。
   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **继承性更新**。 然后，双击您想要更改的策略。
3. 在 **继承性更新策略** 对话框中，选择一个操作系统。 单击 **配置**。
4. 在 **设置更新策略** 对话框，单击 **计划** 标签。 选择 **在拨号连接时作更新检查**。

20.8 指定用于继承性更新的代理服务器

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 更新** 权限，才能配置继承性更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

如果计算机是通过因特网来下载更新文件的，您就必须输入任何您用以连接到因特网的代理服务器的详情。

注: 您要针对各个类型的计算机（如: Windows 2000 及以后），分别输入这些设置。

1. 如果您尚未这样做，请检查您想要配置的计算机组使用的是哪个继承性更新策略。（请参见 查看组采用的策略（第24页）。）在 **策略** 窗格板中，双击 **继承性更新**。 然后，双击您想要更改的策略。 在 **继承性更新策略** 对话框中，选择一个操作系统。 单击 **配置**。
2. 在 **设置更新策略** 对话框，单击 **主服务器** 标签或者，如果需要，单击 **副服务器** 标签。 确保准确无误地输入了所有的详情。 然后，单击 **代理详情**。
3. 在 **代理详情** 对话框中，选择 **通过代理接入服务器**。 然后，输入代理服务器的 **地址** 和 **端口** 号。 输入用来接入代理服务器的 **用户名** 和 **密码**。 如果 “用户名” 需要指明域，才算合格有效。请使用 “域\用户名” 的形式。

20.9 限制带宽使用量

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 更新** 权限，才能配置继承性更新策略。

- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以限制更新所使用的带宽量。这将避免在计算机需要一些带宽以作它用时（如：下载电子邮件），更新工作占用了所有的带宽。

注: 您要针对各个类型的计算机（如：Windows 2000 及以后），分别输入此设置。

1. 如果您尚未这样做，请检查哪个继承性更新策略被您想要配置的计算机组所使用。（请参见 查看组采用的策略（第24页）。）在 **策略** 窗格板中，双击 **继承性更新**。然后，双击您想要更改的策略。在 **继承性更新策略** 对话框中，选择一个操作系统。单击 **配置**。
2. 在 **设置更新策略** 对话框，单击 **主服务器** 标签或者，如果需要，单击 **副服务器** 标签。确保准确无误地输入了所有的详情。然后，单击 **高级**。
3. 在 **高级设置** 对话框中，选择 **限制带宽使用量**，并使用滑动控制条指定以"千字节/每秒"为单位的带宽量。如果您指定的带宽量超过了计算机所能提供的量，更新工作将使用计算机能提供的所有带宽。

20.10 选择不同的初始安装源

如果您使用基于角色的管理，那么，：

- 您必须具备 **策略设置 - 更新** 权限，才能配置继承性更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

依照默认值，防病毒软件安装和不断更新的来源（"主服务器"），是您第一次设置计算机组时所指定的。如果您想从不同的来源进行初始安装，您可以按照以下说明做:

注:

这一设置仅仅应用于 Windows 2000 及以后的计算机上。

如果您的主服务器使用的是 HTTP 地址，而您想从控制台实施安装程序，那么，您必须在此指定初始安装源。

1. 检查您想要配置的计算机组所采用了哪个继承性更新策略。

   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **继承性更新**。然后，双击您想要更改的策略。

3. 在 **设置继承性更新策略** 对话框中，选择一个操作系统，如：Windows 2000 及以后。单击 **配置**。
4. 在 **设置更新策略** 对话框中，单击 **初始安装源** 标签。取消勾选 **使用主服务器地址** 勾选框。然后，输入您想使用的安装源的地址。

20.11 日志记录继承性更新

如果您使用基于角色的管理，那么，：

- 您必须具备 **策略设置 - 更新** 权限，才能配置继承性更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以配置计算机，对其更新活动进行日志记录。

注: 您要针对各个类型的计算机（如：Windows 2000 及以后），分别输入这些设置。

1. 检查您想要配置的计算机组所采用了哪个继承性更新策略。

   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **继承性更新**。然后，双击您想要更改的策略。
3. 在 **继承性更新策略** 对话框中，选择一个操作系统。单击 **配置**。
4. 在 **设置更新策略** 对话框，单击 **日志记录** 标签。确保选择 **记录 Sophos AutoUpdate 活动**。然后，按照以下说明设置其它选项。

   日志文件最大尺寸

   以兆字节（MB）为单位，设定日志文件的最大尺寸。

   日志级别

   您可以选择 **普通记录** 或 **详尽记录** 进行日志记录。详尽的日志记录提供比通常的活动多得多的活动的信息，因而，日志文件的尺寸也会快速增大。请只有在需要用它来处理出现的问题时，才使用这一设置。

20.12 默认的继承性更新目录

如果您在安装 Sophos EM Library 时接受了默认设置，那么，各产品的安装和更新所使用的文件夹，应该如下:

注: 在 “Sophos Endpoint Security and Control” 下载包的目录中包含着针对 Sophos Anti-Virus，Sophos Client Firewall，和 Sophos NAC 等程序的安装程序。

Sophos Endpoint Security and Control for Windows 2000/XP/2003/Vista	\\服务器名称\InterChk\SAVSCFXP
Sophos Anti-Virus for Windows 2000/XP/2003/Vista	\\服务器名称\InterChk\ESXP
Sophos Anti-Virus for Windows NT	\\服务器名称\InterChk\ESNT
Sophos Anti-Virus for Windows 95/98/Me	\\服务器名称\InterChk\ES9x
Sophos Anti-Virus for Mac OS X	\\服务器名称\InterChk\ESOSX
Sophos Anti-Virus for Linux	\\服务器名称\InterChk\savlinux
Sophos Anti-Virus for Windows UNIX	\\服务器名称\InterChk\EESAVUNIX

21 配置防火墙策略

21.1 设置防火墙

依照默认值，防火墙会被启用，并会阻断所有可有可无的通讯流。因此，您应该配置防火墙允许您想要使用的应用程序，并在将它安装到所有的计算机上之前，测试它。要了解更详细的建议，请参见 *Sophos Endpoint Security and Control* 策略设置指南。

要了解有关默认的防火墙设置的信息，请参见 Sophos 技术支持知识库文章 57756 (*http://cn.sophos.com/support/knowledgebase/article/57756.html*)。

要了解更多有关避免网络桥接的信息，请参见 关于设备控制（第138页）。

重要: 当您应用新的或更新的策略到计算机中时，在新的策略被完全应用之前，先前被允许的应用程序可能会被短暂阻断。您应该在应用新的策略之前，告知您的用户此信息。

注: 如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 防火墙** 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多有关基于角色的管理的信息，请参见关于角色和子领域（第11页）。

要使用 **防火墙策略** 向导配置防火墙:

1. 在 **策略** 窗格板中，双击 **防火墙**。

2. 双击 **默认** 策略，以编辑它。

   会出现 **防火墙策略** 向导。

3. 在向导的 **欢迎** 页面中，单击 下一步。

   如果您想要使用高级配置页面，请单击 **高级防火墙策略**。请参见 打开高级配置页（第117页）。

4. 在 **配置防火墙** 页中，选择路径类型:

   - 为总是在网络中的计算机，如: 台式机，请选择 **单一路径**。
   - 如果您想要防火墙，根据计算机使用时的路径，如: 在办公室（网络中）和不在办公室，使用不同的设置，请选择 **双重路径**。您可能会想为笔记型电脑设置双重路径。

5. 如果您在先前的页面中选择了 **双重路径**，请在 **网络识别** 页面中，配置您的网络的 DNS 或 网关识别。

   Enterprise Console 然后将根据它们是否在网络中，来应用不同的防火墙设置。

6. 在 **操作模式** 页面中，选择防火墙将怎样处理流入和流出的通讯流:

模式	描述
阻断流入和流出的通讯流。	■ 默认级别。提供最高级别的安全性。 ■ 只允许必要的通讯流通过防火墙，并且使用检查和认证应用程序。 ■ 要允许在您的公司中常用的应用程序能够通过防火墙进行通讯，请单击 **信任**。要了解更多信息，请参见 关于信任应用程序（第113页）。
阻断流入的通讯流，并允许流出的通讯流。	■ 提供的安全性级别低于 **阻断流入和流出通讯流**。 ■ 允许您的计算机无需您创建特别的规则，就能访问网络和因特网。 ■ 允许所有的应用程序通过防火墙进行通讯。
监控	■ 应用您设置的规则到网络通讯流中。如果通讯流没有匹配规则，它会向控制台报告，并且只允许流出通讯流。 ■ 使您能够收集有关网络的信息，并因此能够在部署防火墙到计算机之前，创建适合的规则。要了解更多信息，请参见 关于使用监控模式（第113页）。
自定义	■ 允许您应用自定义配置。 ■ 单击 **高级**，以配置防火墙策略。要了解有关怎样操作的信息，请参见终结点软件 Sophos Endpoint Security and Control 9.5 的帮助文件中的 “配置防火墙” 部分。

7. 在 **文件和打印机共享** 页中，如果您想要允许计算机共享网络中的本地打印机和文件夹，请选择 **允许文件和打印机共享**。
8. 如果您选择了 **双重路径**，请为副路径（脱网）配置操作模式，文件和打印机共享。

在您设置了防火墙之后，您可以在**防火墙-事件查看器**中查看防火墙事件（如:被防火墙阻断的应用程序）。要了解详情，请参见查看防火墙事件（第60页）。

在最近七日之内，发生事件的数量超过了指定的级别的计算机，同样会显示在指标面板中。

21.2 关于使用监控模式

您可以在供测试的计算机上启用监控模式，并使用“防火墙事件查看器”查看正在使用的是哪些通讯流，应用程序，或线程。

然后，您可以按照创建防火墙规则（第116页）中的说明，使用“事件查看器”创建规则，允许或阻断报告的通讯流，应用程序，和线程。

注: 当您使用“防火墙事件查看器”创建某个规则，并将它添加到防火墙策略中时，防火墙模式会从 **监控** 变为 **自定义**。

提示: 如果您不想默认允许未知的通讯流，您可以使用防火墙学习（交互）模式。请参见 选择学习模式（第115页）。

21.3 关于信任应用程序

为了提高您的计算机的安全性，防火墙会阻断计算机中未能识别的应用程序的通讯流。不过，在您的公司中通常使用的应用程序可能会被阻断，使用户不能进行日常工作。

您可以信任这些应用程序，这样它们就可以通过防火墙进行通讯。受信任的应用程序会被允许进行完全的和无条件的访问网络和因特网。

注: 为了更安全，您可以应用一个或多个应用程序规则到特定的条件中，应用程序须满足该条件才能运行。要了解有关怎样操作的信息，请参见终结点软件 Sophos Endpoint Security and Control 9.5 的帮助文件中的“应用程序规则”部分。

21.4 信任某个应用程序

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 防火墙** 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

要信任某个应用程序:

1. 在 **防火墙策略** 向导的 **操作模式** 页中，在默认模式 **阻断流入和流出的通讯流**。 处于被勾选的状态下，单击 **信任**。
2. 在 **防火墙策略** 对话框中的 **应用程序** 标签页中，单击 **添加**。

3. 在 **防火墙策略 - 添加受信任的应用程序** 对话框的 **事件类型** 文本框中，选择您是想要添加已修改的应用程序，新的应用程序，还是添加在防火墙策略没有为其设置应用程序规则的应用程序。
4. 选择您想要允许信任的应用程序条目。单击 **确定**。

   应用程序已被添加到 **防火墙策略** 对话框中的受信任的应用程序列表中。

5. 在 **防火墙策略** 对话框中，单击 **确定**，以关闭它。
6. 结束 **防火墙策略** 向导。

21.5 允许文件和打印机共享

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 防火墙** 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域 （第11页）。

要允许计算机共享网络中的本地打印机和文件夹:

1. 检查哪个防火墙策略被您想要配置的计算机组所采用了。
   请参见 查看组采用的策略 （第24页）。
2. 在 **策略** 窗格板中，双击 **防火墙**。 然后，双击您想要更改的策略。

   会出现 **防火墙策略** 向导。

3. 请按照向导中的操作指导做。 相应地确认现有的配置，或更改设置。
4. 在 **文件和打印机共享** 页中，选择 **允许文件和打印机共享**。

   注: 此选项与离线（副）路径无关。

5. 结束向导。

21.6 允许已被报告或阻断的应用程序

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 防火墙** 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域 （第11页）。

如果防火墙报告您的联网计算机上发现某个未知的应用程序或阻断某个应用程序，那么，在“防火墙事件查看器”中会显示该事件。 此主题说明怎样从“防

火墙事件查看器”中允许应用程序，以及怎样应用新的规则到您选择的防火墙策略中。

要了解在“防火墙事件查看器”中报告或阻断的应用程序的详情，以及允许它们或为它们创建新的规则：

1. 在 **查看** 菜单中，单击 **防火墙事件**。
2. 在 **防火墙 - 事件查看器** 对话框中，选择想要允许它，或者为它创建规则的应用程序条目。 单击 **创建规则**。
3. 在出现的对话框中，选择是否允许该应用程序，或者，使用现有的预设为它创建规则。
4. 从防火墙策略列表中，选择您想要应用该规则的防火墙策略。 要应用规则到所有策略，选择 **全选**，然后，单击 **确定**。

注： 您还可以使用高级防火墙配置页面，将某应用程序作为可信任的应用程序直接添加防火墙策略中。 请参见 从防火墙策略中创建应用程序规则 （第118页）。

21.7 选择学习模式

如果您使用基于角色的管理，那么，：

- 您必须具备 **策略设置 - 防火墙** 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域 （第11页）。

防火墙可以在学习（交互）模式中工作，询问用户如何处理检测到的通讯流。 在学习模式中，每次未知的应用程序或服务请求网络访问时，防火墙会在终结点计算机上显示一个学习对话框。 学习对话框会询问用户是允许还是阻断通讯流，或者，是否为该类型的通讯流创建规则。

要在计算机组中将防火墙置于学习模式中：

1. 检查哪个防火墙策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略 （第24页）。
2. 在 **策略** 窗格板中，双击 **防火墙**。 然后，双击您想要更改的策略。

   会出现 **防火墙策略** 向导。
3. 在向导的欢迎页面中，单击 **高级防火墙策略** 按钮。

   会出现 **防火墙策略** 对话框。

4. 根据您想要配置的路径，单击相应的 **配置** 按钮。

   会出现 **主路径** 或 **副路径** 对话框。

5. 在 **常规** 标签页的 **工作模式** 下，选择 **交互** 并单击 **确定**。
6. **防火墙策略** 对话框中，单击 **确定**。
7. 结束 **防火墙策略** 向导。

21.8 创建防火墙规则

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 防火墙** 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以为除了“修改了内存”事件之外的所有防火墙事件创建规则。

要创建防火墙规则:

1. 在 **查看** 菜单中，单击 **防火墙事件**。
2. 在 **防火墙 - 事件查看器** 对话框，为您想要为它创建规则的应用程序选择事件，并单击 **创建规则**。
3. 在出现的对话框中，选择您想要应用到应用程序的选项。
4. 选择您想要将该规则应用到哪个路径（主路径，副路径，或两者）。如果您选择应用规则到副路径，或两者，那么，规则只会被添加到配置了副路径的策略中。单击 **确定**。

   注: “新的应用程序”和“修改的应用程序”事件不依赖于路径（它们添加由两个路径共享的检查和）。您不能为这些事件选择路径。

5. 从防火墙策略的列表中，选择您想要应用规则的一个或多个策略。单击 **确定**。

   注: 您不能添加规则到应用于您的活动子领域的之外的策略中。

注: 如果您想要使用高级防火墙策略配置页，直接从防火墙策略创建某个应用程序规则，请参见 从防火墙策略中创建应用程序规则（第118页）。

21.9 临时禁用防火墙

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 防火墙** 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

依照默认值，防火墙是启用的。有时，为了维护或排疑解难，您可能需要暂时禁用防火墙，然后，在重新启用它。

要针对某个计算机组的防火墙:

1. 检查哪个防火墙策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **防火墙**。然后，双击您想要更改的策略。

   会出现 **防火墙策略** 向导。
3. 在向导的欢迎页面，按照以下说明做:
   - 如果您想要关闭所设置的所有路径（主路径和副路径，如果您配置了某一个）中的防火墙，请单击 **下一步**。在 **配置防火墙** 页中，选择 **允许所有通讯流（关闭防火墙）**。结束向导。
   - 如果您想要关闭某一个路径（主路径或副路径）中的防火墙，请单击 **高级防火墙策略** 按钮。在出现的 **防火墙策略** 对话框，选择 **主路径** 或 **副路径** 旁的 **允许所有通讯流**。单击 **确定**。结束 **防火墙策略** 向导。

如果您禁用防火墙，您的计算机将处于非保护状态，直到您重新启用防火墙。要启用防火墙，请取消勾选 **允许所有通讯流** 勾选框。

21.10 使用高级防火墙配置

21.10.1 打开高级配置页

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 防火墙** 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

如果您想要更多地控制防火墙设置，并且能够微调它们，您可以使用高级防火墙策略配置页配置防火墙。

要打开高级防火墙配置页:

1. 双击您想要更改的防火墙策略。
2. 在 **防火墙策略** 向导的欢迎页面中，单击 **高级防火墙策略** 按钮。

   会出现 **防火墙策略** 对话框。在此对话框中，您可以为副路径添加配置，配置路径检测方法，添加应用程序检查和到防火墙策略中，以及配置防火墙日志记录。

3. 在 **防火墙策略** 对话框中，单击您想要配置防火墙的路径旁的 **配置**。

   会出现 **主路径** 或 **副路径** 对话框。在此对话框中，您可以配置将要应用于所选择的路径的选项，例如，过滤 ICMP 消息，允许 LAN 通讯流，添加全局和应用程序规则。

高级防火墙选项的详情，在终结点计算机软件 Sophos Endpoint Security and Control 版本 9 的帮助文件中的“使用 Sophos Client Firewall” 中有具体的说明。以下主题仅说明在 Enterprise Console 中配置与在终结点计算机上配置会有所不同的选项。

- 从防火墙策略中创建应用程序规则（第118页）
- 添加应用程序检查和（第119页）

21.10.2 从防火墙策略中创建应用程序规则

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 防火墙** 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以使用高级防火墙策略配置页，直接从防火墙策略中创建应用程序规则。

要从防火墙策略中创建应用程序规则:

1. 双击您想要更改的策略。
2. 在 **防火墙策略** 向导的欢迎页面中，单击 **高级防火墙策略** 按钮。
3. 在出现的 **防火墙策略** 对话框中，单击您想要配置防火墙的路径旁的 **配置**。

4. 按照以下说明之一做:
   - 如果您想要添加应用程序到防火墙策略，请在出现的对话框中，转到 **应用程序** 标签中，并单击 **添加**。
   - 如果您想要允许应用程序启动隐藏的线程，请转到 **线程** 标签页中，单击位于上方的 **添加**。
   - 如果您想要允许应用程序通过低级插口访问网络，请转到 **线程** 标签页中，单击位于下方的 **添加**。

   会出现 **防火墙策略 - 添加应用程序** 对话框。
5. 如果您是添加应用程序，请在 **事件类型** 文本框中，选择您是添加已修改的应用程序，新的应用程序，还是添加在防火墙策略没有为其设置应用程序规则的应用程序。
6. 选择您想要添加，或想要允许启动隐藏线程，或允许使用低级插口的应用程序的条目，并单击 **确定**。

   该应用程序已被添加到防火墙策略。

如果您在 **应用程序** 标签页中添加应用程序，那么，该应用程序会作为“受信任的”应用程序添加。如果您想要，您可以阻断它，或为它创建自定义规则。

要了解更多有关高级选项的信息，请参见终结点计算机软件 Sophos Endpoint Security and Control 版本 9 的帮助文件中“使用 Sophos Client Firewall”部分。

21.10.3 添加应用程序检查和

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 防火墙** 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域 （第11页）。

每个版本的应用程序都具有独一无二的检查和。防火墙可以使用此检查和决定是否允许某个应用程序。

依照默认值，防火墙会检查每个运行的应用程序的检查和。如果检查和是未知的，或是已被更改，那么，防火墙会阻断它。

要添加检查和到允许的检查和列表中:

1. 双击您想要更改的防火墙策略。
2. 在 **防火墙策略** 向导的欢迎页面中，单击 **高级防火墙策略** 按钮。
3. 在 **防火墙策略** 对话框中，转到 **检查和** 标签页，并单击 **添加**。

4. 在 **防火墙策略 - 添加应用程序检查和** 对话框中的 **事件类型** 文本框中，选择您是想为已更改的应用程序，还是为新的应用程序添加检查和。
5. 选择您想要添加检查和的应用程序条目。 单击 **确定**。

   应用程序检查和已被添加到 **防火墙策略** 对话框中的允许的检查和列表中。

6. 在 **防火墙策略** 对话框中， 单击 **确定**， 以关闭它。
7. 结束 **防火墙策略** 向导。

21.10.4 获取有关高级选项的帮助

要了解所有防火墙选项的完整详情，请参见终结点计算机软件 Sophos Endpoint Security and Control 版本 9 的帮助文件中 “使用 Sophos Client Firewall” 部分。

22 配置应用程序控制策略

22.1 关于应用程序控制

Enterprise Console 使您能够检测和阻断 “受控程序” ， 即：不对计算机安全构成威胁的，正当合法的程序，但是，您认为这些程序不适合在办公环境中使用。 类似的应用程序包括：即时消息(IM)客户端，语音IP电话(VoIP)客户端，数字影像软件，媒体播放器，浏览器插件，等等。

注: 此选项只应用于 Sophos Endpoint Security and Control for Windows 2000 及以后。

凭借充分的灵活性，可以根据不同的计算机组，阻断或批准同样的应用程序。例如，可以阻断办公室计算机上的语音IP电话(VoIP)的应用程序，但是在远程计算机上允许该应用程序。

受控程序列表由 Sophos 提供，并且定期更新。 您不能添加新的应用程序到此列表中，但是，您可以向 Sophos 提交请求，添加您想要在您的网络中控制的非恶意的应用程序。 要了解详情，请参见 Sophos 技术支持知识库文章 35330 (*http://cn.sophos.com/support/knowledgebase/article/35330.html*)。

本节说明怎样选择您想在您的网络中控制的应用程序，以及设置扫描受控程序。

注: 如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 应用程序控制** 权限，才能配置应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多有关基于角色的管理的信息，请参见关于角色和子领域（第11页）。

应用程序控制事件

当某个应用程序控制事件发生时，例如，在网络中检测到某个受控程序，该事件会被记录到应用程序控制事件日志中，并且能够从Enterprise Console中查看它。 要了解详情，请参见 查看应用程序控制事件（第58页）。

在最近七日之内，发生事件的数量超过了指定的级别的计算机，会显示在指标面板中。

您还可以设置当发生应用程序控制事件时，向您选择的收件人发送警报。要了解详情，请参见 设置应用程序控制警报（第154页）。

22.2 选择想要控制的应用程序

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 应用程序控制** 权限，才能配置应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

依照默认值，会允许所有的应用程序。按照以下说明，您可以选择想要控制的应用程序：

1. 检查哪个应用程序控制策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **应用程序控制**。然后，双击您想要更改的策略。
3. 在 **应用程序控制策略** 对话框中，单击 **批准** 标签。
4. 选择某个 **应用程序类型**，例如，**文件共享**。

   包含在该组中的应用程序的完整列表会出现在下面的 **已批准** 列表。

   - 要阻断某个应用程序，请选择该应用程序，并单击“添加”按钮，将它移到 **已阻断** 列表中。

   - 要阻断将来会由 Sophos 添加到此类型中的任何新的应用程序，请移动 **将来全部由 Sophos 添加** 到 **已阻断** 列表中。
   - 要阻断该类型的所有应用程序，请单击“全部添加”按钮，将所有的应用程序从 **已批准** 列表中移到 **已阻断** 列表中。

5. 在 **应用程序控制策略** 对话框的 **扫描** 标签中，确保启用了扫描受控程序。（详情请参见 扫描想要控制的应用程序（第122页）。）单击 **确定**。

22.3 扫描想要控制的应用程序

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 应用程序控制** 权限，才能配置应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以配置 Sophos Endpoint Security and Control 读写扫描您想在网络中控制的应用程序。

1. 检查哪个应用程序控制策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **应用程序控制**。 然后，双击您想要更改的策略。

   会出现 **应用程序控制策略** 对话框。
3. 在 **扫描** 标签中，按照以下说明设置选项:
   - 要启用读写扫描，请勾选 **启用读写扫描** 勾选框。 如果您想要在读写时检测应用程序，但是不想阻断它们，请选择 **检测但允许运行** 勾选框。
   - 要启用即时和计划扫描，请勾选 **启用即时和计划扫描** 勾选框。

   注: 您的防病毒和 HIPS 策略设置，将决定哪些文件会被扫描（即：扩展名和排除项目）。

如果您想要删除在联网计算机上发现的受控程序，请按照 卸载不想要的受控程序（第122页） 中的指导说明做。

如果组中的任何一台计算机中出现受控程序，您还可以向特定的用户寄送警报。 要了解操作指导，请参见 设置应用程序控制警报（第154页）。

22.4 卸载不想要的受控程序

在您卸载受控程序之前，请确保已禁用读写扫描受控程序功能。 这种类型的扫描会阻断用于安装和卸载应用程序的程序，所以它会干扰卸载过程。

您可以使用两种方法删除某个应用程序:

- 到各台计算机上，运行卸载程序，卸载该软件产品。 您通常可以使用 Windows 控制面板中的“添加/删除程序”来实现这一点。
- 在服务器上，使用脚本程序或管理工具，运行卸载程序，卸载联网计算机上的该软件产品。

现在您可以启用读写扫描受控程序了。

23 配置数据控制策略

23.1 关于数据控制

数据控制，通过监控和限制传输包含敏感数据的文件，使您能够减少从工作站计算机意外丢失数据的机会。 您通过创建各种数据控制规则，并将这些规则添加到**数据控制**策略中，来进行数据控制。

您可以监控传输到特定的存储设备（如: 移动存储设备或光驱）的文件，或监控通过特定的应用程序（如: 电子邮件客户端或网页浏览器）传输的文件。

为了使您能够迅速定义和部署数据控制策略，SophosLabs 提供了一个敏感数据定义库（内容控制列表(Content Control List)）。 这个库主要集中于个人身份识别信息，不过，它也保护其它常用的数据结构。 您可以按照本节中的进一步的说明，在 Enterprise Console 中使用内容控制列表 (Content Control List)。

23.2 数据控制怎样工作？

数据控制，可以识别意外的数据丢失，这通常是由职员不当处理敏感数据造成。例如，用户通过基于网页的电子邮件将包含敏感数据的文件寄回家。

数据控制使您能够监控从计算机到存储设备和连接到因特网的应用程序的文件传输。

- **存储设备** 数据控制会介入分析通过“资源管理器”（包括 Windows 桌面）复制到受控的存储设备的所有文件。不过，直接在应用程序（如: Microsoft Word）内部进行的复制，或者，使用命令行提示窗进行的传输，不会被介入分析。

  通过 **允许用户接受的传输和日志事件** 措施选项，或 **阻断传输和日志事件** 措施选项，可以强制所有向受控的存储设备进行的传输，都要使用“资源管理器”进行。任何直接在应用程序内部进行的保存，或者，使用命令行提示窗进行的文件传输，这两种情况都会被数据控制阻断；并且会向用户显示桌面警报，要求他们使用“资源管理器”完成传输。

当数据控制策略只包含具有 **允许文件传输和日志事件** 措施选项时，任何直接在应用程序内部进行的保存，或者，使用命令行提示窗进行的文件传输，不会被介入分析。这会使用户能够不受限制地使用存储设备。不过，使用“资源管理器”进行的传输，仍然会作为数据控制事件被日志记录。

注: 此限制不会应用于应用程序控制。

- **应用程序** 为确保只监控用户上传的文件，某些系统文件路径会从数据控制监控中排除。这将显著地减少由应用程序开启配置文件生成数据控制事件，而不用户上传文件生成数据控制事件的情况。

重要: 如果您遇到错误地由某应用程序开启配置文件而生成事件的情况，解决此问题的通常是添加自定义的排除路径，或配置数据控制规则减低敏感度。要了解更多信息，请参见技术支持知识库文章 63016 (*http://cn.sophos.com/support/knowledgebase/article/63016.html*)。

数据控制策略

数据控制使您能够通过定义数据控制策略和应用这些策略到您的网络中的计算机组中，来监控文件的传输活动。

重要: 数据控制不支持 Windows 2008 Server Core，并且必须在运行此操作系统的计算机上被禁用。要从数据控制扫描中排除 Windows 2008 Server Core 计算机，请将这些计算机放置到具有禁用数据控制扫描的数据控制策略的计算机组中。要了解详情，请参见 开启或关闭数据控制（第128页）。

数据控制策略包括一个或多个数据控制规则，这些规则指定数据控制将要检测的条件，以及当规则被匹配使将要采取的措施。一个数据控制规则可以被包括在多个策略中。

在某个数据控制策略中包含多个规则时，某文件只要匹配该数据控制策略中的任一规则，就会被视为违反了该策略。

数据控制规则条件

数据控制规则条件包括目标路径，文件名及其扩展名，或文件内容。

目标路径包括设备（例如，类似 USB 闪存的移动存储设备）和应用程序（例如，因特网浏览器和电子邮件客户端程序）。

文件内容的匹配是通过内容控制列表 (CCL) 来定义的。内容控制列表 (CCL) 是基于 XML 的结构化数据描述。SophosLabs 提供了一个内容控制列表 (CCL) 的扩展集，它可以用于您的数据控制规则中。

要了解更多有关应用数据控制规则和条件到文件中的信息，请参见 关于数据控制规则（第126页）。

要了解更多有关定义文件内容的内容控制列表(CCL)的信息，请参见关于内容控制列表（第126页）。

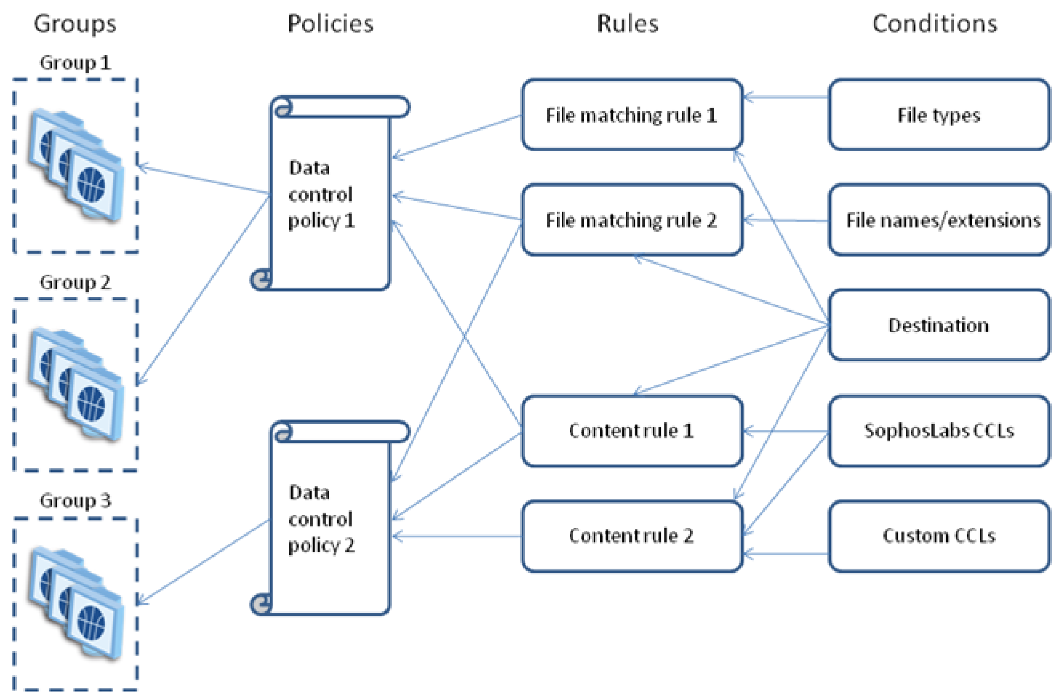


图5：数据控制

数据控制规则措施

当数据控制检测到在规则中指定的所有条件时，即为规则被匹配，则数据控制将采取在规则中指定的措施，并将此事件记录到日志中。您可以指定以下措施之一:

- 允许文件传输和日志事件
- 允许用户接受的传输和日志事件
- 阻断传输和日志事件

如果某文件匹配指定了不同措施的两条数据控制规则，那么，指定的措施最严格的规则将被应用。阻断文件传输的数据控制规则的优先性，高于允许用户接受的文件传输的数据控制规则。允许用户接受的文件传输的数据控制规则的优先性，高于允许文件传输的数据控制规则。

依照默认值，当规则被匹配后文件的传输被阻断时，或者，当要求用户确认文件的传输时，会有消息出现在终结点计算机的桌面上。被匹配的规则，会在消

息中指出。您可以添加您自定义的消息到，供用户确认文件传输和阻断文件传输所使用的标准消息中。要了解更多信息，请参见 设置数据控制警报（第155页）。

23.3 关于数据控制规则

数据控制规则指定数据控制将检测的条件，指定当规则被匹配时，将采取的措施，以及指定您或许想从数据控制扫描中排除的文件。

您可以创建自己的规则或使用 Sophos 提供的数据控制规则样本。 Sophos 提供了一些预先配置的数据控制规则，您可以现成地使用它们，也可以修改它们满足您的需要。 这些规则只作为范例提供，Sophos 并不更新它们。

有两种类型的数据控制规则： 文件匹配规则 和 内容规则。

文件匹配规则

文件匹配规则，是如果当用户试图传输具有某些特定的文件名或特定的文件类型（真实的文件类型类别，如：电子表格文件）的文件到特定的路径时，指定所要采取的措施的规则。例如，阻断传输数据库文件到移动存储设备。

数据控制包括针对 150 多个文件格式的真实文件类型的定义。 Sophos 可能会添加更多的真实文件类型，以便使数据控制可以检测它们。 新添加的文件类型，将被自动添加到所有使用该相关的真实文件类型类别的数据控制规则中。

没有包括在真实文件类型定义中的文件类型，可以通过它们的文件扩展名来识别。

内容规则

内容规则，是包括一个或多个内容控制列表，并指定，如果用户试图传输匹配了规则中的全部内容控制列表的数据到指定目标路径 (destination) 时，指定所要采取的措施的规则。

23.4 关于内容控制列表

内容控制列表 *(CCL)*，是描述结构化的文件内容的条件集合。 内容控制列表 (Content Control List) 可能描述单一的数据类型（例如，家庭住址或社会保险号），或者，描述各种数据类型组合（例如，几乎等同于“机密”二字的某个项目名称）。

您可以使用 Sophos 提供的 *SophosLabs Content Control Lists*，或创建您自己的内容控制列表。

SophosLabs Content Control Lists 提供针对常用的财务和个人身份识别数据类型（例如，信用卡好，社会保险号，家庭住址，或电子邮件地址等）的专业定义。诸如总和检查等，高级技巧被用于 SophosLabs Content Control Lists 之中，增加了检测敏感数据的精确性。

您不能够编辑 SophosLabs Content Control Lists，但是您可以提交请求给 Sophos，要求创建新的 SophosLabs Content Control List。要了解详情，请参见 Sophos 技术支持知识库文章 51976 (*http://cn.sophos.com/support/knowledgebase/article/51976.html*)。

注: 当前版本的内容控制列表(CCL)不保证支持双字节字符（例如，日语或中文字符）。不过，您可以在内容控制列表(CCL)编辑器中输入双字节字符。

为 SophosLabs Content Control Lists 设置数量

大多数的 SophosLabs Content Control Lists 都被指派了数量。

数量，是在内容控制列表被匹配之前，必须在文件中找到的内容控制列表 (CCL) 的键数据类型 (key data type) 的数量。您可以在包含内容控制列表 (CCL) 的内容规则中编辑 SophosLabs Content Control List 的数量值。

使用数量，您可以微调数据控制规则，从而避免阻断并不包含敏感信息的文件（例如，在信头或签名中，可能包含邮寄地址或一个或两个电话号码的文件）。如果您只是单一地查找邮寄地址，那么，会有成千个文件匹配规则，并触发数据控制事件。但是，如果您想要避免流失客户名单，您可能会检测所传输的文件中包含，比如，50 个以上的邮寄地址的文件。不过，在其它情况下，建议您单一地查找内容实体，比如，信用卡号。

23.5 关于数据控制事件

当发生数据控制事件时，例如，复制包含敏感数据的文件到USB闪存中，该事件会被发送到 Enterprise Console 中，并且可以在 **数据控制 - 事件查看器** 中查看它。该事件还会被日志记录到本地的终结点计算机上，并且在具有相应的权限的情况下，可以在 Sophos Endpoint Security and Control 中查看它。

注: 一个终结点计算机每小时最多可以向 Enterprise Console 发送 50 个数据控制事件。所有的事件都会日志记录到本地的终结点计算机上。

在 **数据控制 - 事件查看器** 对话框中，您可以使用筛选挑选仅仅显示您感兴趣的事件。您还可以将数据控制事件列表导出到文件中。要了解详情，请参见“查看事件”部分。

在最近七日之内，发生数据控制事件的数量超过了指定的级别的计算机，会显示在指标面板中。要了解怎样设置级别的信息，请参见 配置指标面板（第 47页）。

您还可以设置当发生数据控制事件时，向您选择的收件人发送警报。要了解详情，请参见 设置数据控制警报（第155页）。

23.6 开启或关闭数据控制

如果您使用基于角色的管理，那么，：

- 您必须具备 **策略设置 - 数据控制** 权限，才能配置数据控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

依照默认值，数据控制是关闭的，并且没有指定任何规则监控或限制网络中的文件传输。

要开启数据控制:

1. 请检查您想要配置的计算机组使用的是哪个数据控制策略。

   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **数据控制**。 然后，双击您想要更改的策略。

   会出现 **数据控制策略** 对话框。
3. 在 **策略规则** 标签页中，勾选 **启用数据控制扫描** 勾选框。
4. 单击 **添加规则** 按钮。 在 **数据控制规则管理** 对话框中，选择您想要添加到策略中的规则，并单击 **确定**。

   重要: 在您添加任何数据控制规则之前，数据控制将不会监控或限制任何文件传输。

如果您稍后想要禁用数据控制扫描，请取消勾选 **启用数据控制扫描** 勾选框。

23.7 创建文件匹配规则

如果您使用基于角色的管理，那么，：

- 您必须具备 **数据控制 - 自定义** 权限，才能创建或编辑数据控制规则。
- 您必须具备 **策略设置 - 数据控制** 权限，才能设置数据控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

要了解文件匹配规则概述，请参见 关于数据控制规则（第126页）。

要创建文件匹配规则，并将它添加到数据控制策略中：

1. 请检查您想要配置的计算机组使用的是哪个数据控制策略。

   请参见 查看组采用的策略（第24页）。

   或者，您可以从**工具**菜单创建规则，并稍后将它添加到一个或多个策略中。在 **工具** 菜单中，指向 **管理数据控制**，然后，单击 **数据控制规则**，然后，执行步骤 4 到步骤 10。

2. 在 **策略** 窗格板中，双击 **数据控制**。 然后，双击您想要更改的策略。
3. 在 **数据控制策略** 对话框的 **策略规则** 标签页中，确保已勾选 **启用数据控制扫描** 勾选框，然后，单击 **管理规则**。
4. 在 **数据控制规则管理** 对话框中，单击 **添加文件匹配规则** 按钮。
5. 在 **创建文件匹配规则** 对话框中的 **规则名称** 下，输入规则的名称。
6. 在 **规则描述（可选）** 中，如果您需要，输入对规则的描述。
7. 在 **选择规则规则的条件** 中，为规则选择条件。

   目标路径条件是预先选择的，并且必须包括在规则中。

   依照默认值，所有的文件类型都会被扫描。 如果您只想扫描某些特定的文件类型，请选择 **当文件类型为**。 然后，您可以按照步骤 10 中的说明，设置此条件。

8. 在 **选择如果匹配规则时，将采取的措施。**，选择措施。
9. 如果您想要从数据控制扫描中排除某些文件，请在 **选择要排除的文件** 下，勾选 **当文件名匹配** 或 **当文件类型为** 勾选框。

10. 在 **规则内容** 下，单击各个下划线的值，并设置规则的条件。
    例如，如果您单击 **选择目标路径**，**匹配目标类型条件** 对话框会开启，您可以在对话框中选择想要限制数据传输的设备和/或应用程序。

    为各个下划线的值选择或输入条件。

    单击 **确定**。

    新的规则会出现在 **数据控制规则管理** 对话框中。

11. 要添加规则到策略中，请勾选规则名称旁的勾选框，并单击 **确定**。

    该规则会被添加到数据控制策略。

您可以设置当数据控制策略中的规则被匹配时，发送给用户的警报和消息。请参见 设置数据控制警报（第155页）。

23.8 创建内容规则

如果您使用基于角色的管理，那么，:

- 您必须具备 **数据控制 - 自定义** 权限，才能创建或编辑数据控制规则和内容控制列表 (CCL)。
- 您必须具备 **策略设置 - 数据控制** 权限，才能设置数据控制策略。

- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

要了解内容规则和内容控制列表概述，请参见关于数据控制规则（第126页）。

要创建内容规则，并将它添加到数据控制策略中：

1. 请检查您想要配置的计算机组使用的是哪个数据控制策略。

   请参见 查看组采用的策略（第24页）。

   或者，您可以从**工具**菜单创建规则，并稍后将它添加到一个或多个策略中。在 **工具** 菜单中，指向 **管理数据控制**，然后，单击 **数据控制规则**，然后，执行步骤 4 到步骤 13。
2. 在 **策略** 窗格板中，双击 **数据控制**。 然后，双击您想要更改的策略。
3. 在 **数据控制策略** 对话框的 **策略规则** 标签页中，确保已勾选 **启用数据控制扫描** 勾选框，然后，单击 **管理规则**。
4. 在 **数据控制规则管理** 对话框中，单击 **添加内容规则** 按钮。
5. 在 **创建内容规则** 对话框的 **规则名称** 下，输入规则的名称。
6. 在 **规则描述（可选）** 中，如果您需要，输入对规则的描述。
7. 在 **选择规则的条件**， 文件内容和目标路径条件已被选择。 您必须为内容规则设置这两种条件。
8. 在 **选择如果匹配规则时，将采取的措施**。， 选择措施。
9. 如果您想要从数据控制扫描中排除某些文件，请在 **选择要排除的文件** 下，勾选 **当文件名匹配** 或 **当文件类型为** 勾选框。
10. 在 **规则内容** 下，单击“选择文件内容”下划线值。
11. 在**内容控制列表管理**对话框中，选择您想要包括在规则中的内容控制列表。

    如果您想要添加 SophosLabs Content Control List，请选择针对您的国家所应用的那个内容控制类表，或者，选择针对全局的内容控制列表。

    如果您想要创建新的内容控制列表，请参见 *创建或编辑简单内容控制列表 (CCL)*（第135页） 或 *创建或编辑高级内容控制列表*（第136页）。

    单击 **确定**。
12. 如果您想要更改指派给 SophosLabs Content Control List 的数量，请在 **规则内容** 下，单击您想要更改的“数量”下划线值（ “*n* 或更多的匹配” ）。 在 **数量编辑器** 对话框中，输入新的数量值。

13. 在 **规则内容** 下，选择或输入剩下的下划线值的条件。

创建内容规则

1. 规则名称 (N):

国际银行帐号号码

2. 规则描述(可选) (D):

识别包含国际银行帐号号码的文档。

3. 选择规则的条件 (C):

当文件包含

当目标路径为

4. 选择如果匹配规则时，将采取的措施 (A):

允许文件传输和日志事件

允许用户接受的传输和日志事件

阻断传输和日志事件

5. 选择要排除的文件 (E):

当文件名匹配

当文件类型为

6. 规则内容 (R):

针对任何文件

当文件 包含：，

10 或更多的匹配 / International Bank Account Numbers [Global]，

和当目标路径为

光盘驱动器

或 可移动存储设备

确定 取消

单击 **确定**。

新的规则会出现在 **数据控制规则管理** 对话框中。

14. 要添加规则到策略中，请勾选规则名称旁的勾选框，并单击 **确定**。

该规则会被添加到数据控制策略。

您可以设置当数据控制策略中的规则被匹配时，发送给用户的警报和消息。请参见 设置数据控制警报（第155页）。

23.9 添加数据控制规则到策略中

如果您使用基于角色的管理，那么，：

- 您必须具备 **策略设置 - 数据控制** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

要添加数据控制到策略中：

1. 请检查您想要配置的计算机组使用的是哪个数据控制策略。
   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **数据控制**。 然后，双击您想要更改的策略。
   会出现 **数据控制策略** 对话框。
3. 在 **策略规则** 标签页中，单击 **添加规则**。
   会出现 **数据控制规则管理器** 对话框。
4. 请选择您想要添加到策略中的规则，并单击 **确定**。

23.10 从策略中删除数据控制规则

如果您使用基于角色的管理，那么，：

- 您必须具备 **策略设置 - 数据控制** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

要从策略中删除数据控制规则：

1. 请检查您想要配置的计算机组使用的是哪个数据控制策略。
   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **数据控制**。 然后，双击您想要更改的策略。
   会出现 **数据控制策略** 对话框。
3. 在 **策略规则** 标签页中，选择您想要删除的规则，然后，单击 **删除规则**。

23.11 从数据控制中排除文件或文件类型

如果您使用基于角色的管理，那么，您必须具备 **数据控制 - 自定义** 权限，才能从数据控制中排除文件。 要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以通过在数据控制规则中，设置排除项目来从数据控制中排除文件和文件类型。

要从数据控制中排除文件或文件类型，请在规则中排除它，并赋予最高的优先级（即：指定最严格的限制措施）。

要从数据控制中排除文件或文件类型：

1. 在 **工具** 菜单中，指向 **管理数据控制**，然后，单击 **数据控制规则**。
2. 在 **数据控制规则管理** 对话框中，选择您想要编辑的规则，并单击 **编辑**，或者，通过单击 **添加文件匹配规则** 或 **添加内容规则** 按钮，创建新的规则。
3. 要从数据控制中排除文件，请在 **规则编辑器** 对话框的 **选择要排除的文件** 下，勾选 **当文件名匹配** 勾选框。
4. 在 **规则内容** 下，单击下划线值以指定被排除的文件的名称。
5. 在 **排除文件名条件** 对话框中，单击 **添加** 并指定您想要排除的文件的名称。

   您可以使用通配符 * 和 ?

   通配符?只能用于文件名或文件扩展名中。一般地，它可以匹配任何单一的字符。然而，在文件名或扩展名的最后使用通配符时，它匹配单个字符，或者，不匹配字符。例如：file??.txt 可以匹配 file.txt，file1.txt 和 file12.txt，但是不匹配 file123.txt。

   通配符 * 仅能以 [filename].* 或 *.[extension] 的形式用于文件名或扩展名中。比如，file*.txt，file.txt* 及 file.*txt 是无效的。
6. 要从数据控制中排除文件类型，请在 **规则编辑器** 对话框的 **选择要排除的文件** 下，勾选 **当文件类型为** 勾选框。
7. 在 **规则内容** 下，单击下划线值以指定被排除的文件类型。
8. 在 **排除文件类型条件** 对话框中，选择您想要排除的文件类型，并单击 **确定**。

23.12 导入或导出数据控制规则

如果您使用基于角色的管理，您必须具备 **数据控制 - 自定义** 权限，才能导入或导出数据控制规则。要了解更多信息，请参见关于角色和子领域（第11页）。

数据控制规则可以作为 XML 文件导入或导出 Enterprise Console。

要导入或导出数据控制规则：

1. 在 **工具** 菜单中，指向 **管理数据控制**，然后，单击 **数据控制规则**。
2. 在 **数据控制规则管理** 对话框中，单击 **导入** 或 **导出**。
   - 如果您想导入规则，请在 **导入** 对话框中，浏览找到您想要导入的规则，选择它并单击 **打开**。
   - 如果您想导出规则，请在 **导出** 对话框中，浏览找到将要保存导出文件的目标路径，输入文件的名称，并单击 **保存**。

23.13 创建或编辑简单内容控制列表 (CCL)

如果您使用基于角色的管理，那么，您必须具备**数据控制-自定义**权限，才能创建内容控制列表 (CCL)。 要了解更多信息，请参见 关于角色和子领域（第11页）。

要了解内容控制列表 (CCL) 概述，请参见 关于内容控制列表（第126页）。

要创建或编辑内容控制列表 (CCL)

1. 在**工具**菜单中，指向**管理数据控制**，然后，单击**数据内容控制列表(CCL)**。
2. 在**内容控制列表管理**对话框中，单击**添加**以创建新的内容控制列表(CCL)，或者，选择某个现有的内容控制列表 (CCL)，并单击 **编辑**。
3. 在 **添加内容控制列表** 对话框的 **名称** 栏中，输入内容控制列表 (CCL) 的名称。
4. 在 **描述** 栏中，如果您需要，输入对内容控制列表 (CCL) 的描述。
5. 如果您想要添加标识或编辑指定给内容控制列表 (CCL) 的标识，请单击 **标识** 栏旁的 **更改** 按钮。

   您可以指派标识，以识别内容控制列表 (CCL) 的类型和它所应用的地区。
6. 在 **编辑内容控制列表标识** 对话框的 **可用标识** 列表中，选择您想要指派的标识，并将它们移动到 **已选择的标识** 列表中。 单击 **确定**。
7. 在 **扫描内容匹配** 部分，选择某个搜索条件（ “任何这些条件”， “所有这些条件”，或 “完全匹配此表达” ），并输入您想在文档中找到的搜索词，使用空格分隔。 单击 **确定**。

   注: 搜索词是区分大小写的。

   简单内容控制列表 (CCL) 不支持使用引号。 请使用 “完全匹配此表达” 条件，扫描完全一致的表达。

   要创建更复杂的表达式，请按照 创建或编辑高级内容控制列表（第136页）中的说明，使用高级内容控制列表 (CCL) 编辑器。

新的内容控制列表会出现在 **内容控制列表管理** 对话框中。

示例

搜索条件	示例	描述
匹配任何条件	机密	匹配包含 “机密” 或 “秘密” 字样的文档。

搜索条件	示例	描述
匹配所有条件	项目机密	匹配包含“项目”和“机密”字样的文档。
完全匹配	仅供内部使用	匹配包含“仅供内部使用”字样的文档。

现在，您可以将此新建的内容控制列表 (CCL) 添加到内容规则中。

23.14 创建或编辑高级内容控制列表

如果您使用基于角色的管理，那么，您必须具备**数据控制-自定义**权限，才能创建内容控制列表 (CCL)。要了解更多信息，请参见关于角色和子领域（第11页）。

要了解内容控制列表 (CCL) 概述，请参见关于内容控制列表（第126页）。

您可以创建包含一个或多个正则表达式和触发积分的内容控制列表(CCL)。要这样做，请使用高级编辑器。

要使用高级编辑器创建或编辑内容控制列表 (CCL):

1. 在**工具**菜单中，指向**管理数据控制**，然后，单击**数据内容控制列表(CCL)**。
2. 在**内容控制列表管理**对话框中，单击**添加**以创建新的内容控制列表(CCL)，或者，选择某个现有的内容控制列表 (CCL)，并单击**编辑**。
3. 在**添加内容控制列表**对话框的**名称**栏中，输入内容控制列表 (CCL) 的名称。
4. 在**描述**栏中，如果您需要，输入对内容控制列表 (CCL) 的描述。
5. 如果您想要添加标识或编辑指定给内容控制列表 (CCL) 的标识，请单击**标识**栏旁的**更改**按钮。

   您可以指派标识，以识别内容控制列表 (CCL) 的类型和它所应用的地区。
6. 在**编辑内容控制列表标识**对话框的**可用标识**列表中，选择您想要指派的标识，并将它们移动到**已选择的标识**列表中。单击**确定**。
7. 单击**高级**按钮。
8. 在**高级**窗格板，单击**创建**以创建新的表达式，或者，选择某个现有的表达式，然后，单击**编辑**。
9. 在**内容控制列表-高级**对话框中，输入 Perl 5 正则表达式。

   要了解 Perl 5 正则表达式的说明，请参见 Perl 技术文档或访问 *http://www.boost.org/doc/libs/1_34_1/libs/regex/doc/syntax_perl.html*。

10. 在 **表达式积分** 栏中，输入当满足正则表达式时，需要添加到内容控制列表 (CCL) 中的总积分的积分数。
11. 在 **最大计数** 栏中，输入可以添加到总计中的最多的匹配正则表达数。
    例如，某个具有 5 分以及最大计数为 2 的表达式，将添加最多10分到内容控制列表 (CCL) 的总计积分中。 如果该表达式被发现 3 次，它仍然是添加 10 分到总计积分中。

    单击 **确定**。
12. 如果您想添加更多的正则表达式到内容控制列表 (CCL) 中，请重复步骤 5 到步骤 11。
13. 在 **触发积分** 栏中，输入在匹配内容控制列表之前，正则表达式必须被匹配的次数。

    例如，设想某个内容控制列表的触发积分为 8，并且由 3 个表达式（A，B，和 C）组成，它们具有以下的积分和最大计数：

表达式	积分	最大计数
表达式 A	5	2
表达式 B	3	1
表达式 C	1	5

    如果数据控制发现 2 个表达式 A 的匹配，或者，发现 1 个表达式 A 的匹配，和 1 个表达式 B 的匹配，或者，1 个表达式 B 的匹配，和 5 个表达式 C 的匹配，那么，此内容控制列表 (CCL) 则被匹配。

    单击 **确定**。

新的内容控制列表 (CCL) 会出现在 **内容控制列表管理** 对话框中。

正则表达式示例

(?i)\b[a-ceghj-pr-tw-z][a-ceghj-npr-tw-z]\s?\d{2}\s?\d{2}\s?\d{2}\s?[abcd]?\b

此正则表达式匹配社会保险号号，例如，AA 11 11 11 A.

(?i)	使匹配区分大小写。
\b	匹配某个字符符号和非字符符号之间的边界值。
[a-ceghj-pr-tw-z]	匹配字符范围（A 到 C E G H J 到 P R 到 T W 到 Z）中的任一单一字符。

?	匹配前置元素 (preceding element) 零次或一次。
\s?	匹配零或一个空白(whitespace)。
\d{2}	匹配两个数位。
[abcd]	匹配列表（A，B，C，或 D）中的任何单个字符。

现在，您可以将此新建的内容控制列表 (CCL) 添加到内容规则中。

23.15 导入或导出内容控制列表 (CCL)

如果您使用基于角色的管理，您必须具备 **数据控制 - 自定义** 权限，才能导入或导出内容控制列表 (CCL)。 要了解更多信息，请参见 关于角色和子领域（第 11页）。

内容控制列表 (CCL) 可以作为 XML 文件导入或导出 Enterprise Console。 您可以在支持内容控制列表 (CCL) 的 Sophos 产品之间共享内容控制列表 (CCL)。

注: SophosLabs Content Control List 无法被导出。

要导入或导出内容控制列表 (CCL):

1. 在 **工具** 菜单中，指向 **管理数据控制**，然后，单击 **数据控制内容控制列表**。
2. 在 **内容控制列表管理** 对话框中，单击 **导入** 或 **导出**。
   - 如果您想导入内容控制列表 (CCL)，请在 **导入** 对话框中，浏览找到您想要导入的内容控制列表 (CCL)，选择它并单击 **打开**。
   - 如果您想导出内容控制列表 (CCL)，请在 **导出** 对话框中，浏览找到将要保存导出文件的目标路径，输入文件的名称，并单击 **保存**。

24 配置设备控制策略

24.1 关于设备控制

重要: Sophos 设备控制不应该与其它软件供应商的设备控制软件共同部署。

设备控制可以使您防止用户在他们的计算机上，使用未经批准的外部硬件设备，移动存储介质，以及无线连接技术。 这能够极大地降低您意外流失数据的风险，限制用户将外来软件安装到网络中的能力。

移动存储设备，光盘启动器，以及软盘驱动器还可以被设置为仅提供只读访问。

使用设备控制，您还可以显著降低公司网络和非公司网络之间的网络桥接风险。**阻断桥接**模式可用于无线和调制解调类型的设备。此模式的工作方式为，当某终结点计算机（通常是通过以太网连接的方式）连接到物理网络时，则禁用无线或调制解调网络适配器。一旦终结点计算机与物理网络断开了连接，无线或调制解调网络适配器会顺畅地重新启用。

依照默认值，设备控制是关闭的，所有的设备都会被允许。

如果您想首次启用设备控制，Sophos 建议您：

- 选择要控制的设备类型。
- 检测但不阻断它们。
- 通过设备控制事件来决定阻断哪些设备类型，以及或许要免除的设备。
- 检测并阻断设备，或者，允许只读访问存储设备。

要了解更多有关针对设备控制的建议设置，请参见 *Sophos Endpoint Security and Control* 策略设置指南。

注: 如果您使用基于角色的管理，那么，：

- 您必须具备 **策略设置 - 设备控制** 权限，才能配置应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

24.2 关于设备控制事件

当发生设备控制事件时，例如，某移动存储设备被阻断，该事件会被发送到 Enterprise Console 中，并且可以在 **设备控制 - 事件查看器** 对话框中查看它。

在 **设备控制-事件查看器** 对话框中，您可以使用筛选挑选仅仅显示您感兴趣的事件。您还可以将设备控制事件列表导出到文件中。要了解详情，请参见“查看事件”部分。

您可以通过设备控制事件，将特定的设备或设备型号作为免除项目添加到设备控制策略中。要了解更多有关免除设备的信息，请参见 从单个策略中免除设备（第144页） 或 从所有策略中免除设备（第143页）。

在最近七日之内，发生设备控制事件的数量超过了指定的级别的计算机，会显示在指标面板中。要了解怎样设置级别的信息，请参见 配置指标面板（第47页）。

您还可以设置当发生设备控制事件时，向您选择的收件人发送警报。要了解详情，请参见 设置设备控制警报（第156页）。

24.3 可以控制什么类型的设备?

设备控制可以使您阻断三种类型的设备：存储设备，网络设备，以及短距设备 *(short range)*。

存储

- 可移动存储设备（如：USB 闪存，PC 读卡器，以及外置硬盘）
- 光学介质驱动器（CD-ROM/DVD/Blu-ray 驱动器）
- 软盘驱动器
- 安全的可移动存储设备（SanDisk Cruzer Enterprise，SanDisk Cruzer Enterprise FIPS Edition，Kingston Data Traveler Vault - Privacy Edition，Kingston Data Traveler BlackBox，以及具有硬件加密的 IronKey Enterprise Basic Edition USB 闪存）

通过使用安全的可移动存储分类，您可以在阻断其它可移动存储设备的同时，方便地允许使用受到支持的安全的可移动存储设备。要了解所支持的安全移动存储设备的最新列表，请参见 Sophos 技术支持知识库文章 63102 (*http://cn.sophos.com/support/knowledgebase/article/63102.html*)。

网络

- 调制解调器
- 无线连接（Wi-Fi 接口，802.11 标准）

对于网络接口，您还可以选择 **阻断桥接** 模式，以帮助您显著降低公司网络和非公司网络之间的网络桥接风险。此模式的工作方式为，当某终结点计算机（通常是通过以太网连接的方式）连接到物理网络时，则禁用无线或调制解调网络适配器。一旦终结点计算机与物理网络断开了连接，无线或调制解调网络适配器会顺畅地重新启用。

短距 (short range)

- 蓝牙接口
- 红外接口（(IrDA 红外接口）

设备控制会同时阻断内置和外置的设备和接口。例如，某个阻断蓝牙接口的策略，将会阻断以下两者:

- 计算机中内建的蓝牙接口
- 任何通过 USB 接入计算机的蓝牙适配器

24.4 选择要控制的设备类型。

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 设备控制** 权限，才能编辑应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域 (第11页) 。

重要: 您不应该阻断 Enterprise Console 通过 Wi-Fi 来进行管理的计算机上的 Wi-Fi 连接。

1. 检查哪个设备控制策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略 (第24页) 。
2. 在 **策略** 窗格板中，双击 **设备控制**。 然后，双击您想要更改的策略。
3. 在 **设备控制策略** 对话框中 **配置** 标签页的 **存储** 下，选择您想要控制的存储设备的类型。
4. 单击设备类型旁的 **状态** 栏，然后，单击出现的下拉箭头。 选择您想要允许的访问权限类型。

   依照默认值，设备具有完全访问权限。 对可移动的存储设备，光盘驱动器，和软盘驱动器，您可以更改它们为 “已阻断” 或 “只读” 。 对安全的可移动的存储设备，您可以更改它为 “已阻断” 。
5. 在 **网络** 下，选择您想要阻断的网络设备的类型。
6. 单击网络设备类型旁的 **状态** 栏，然后，单击出现的下拉箭头。
   - 勾选 “阻断” ，如果您想要阻断该设备类型。
   - 勾选 “阻断桥接” ，如果您想要避免公司网络和非公司网络之间的网络桥接。 当某终结点计算机 (通常是通过以太网连接的方式) 连接到物理网络时，该设备类型会被阻断。 一旦终结点计算机与物理网络断开了连接，该设备类型会重新启用。
7. 在 **短距** 下，勾选您想要阻断的短距设备的类型。 在设备类型旁的 **状态** 栏中，选择 “已阻断” 。

   单击 **确定**。

24.5 检测设备但不阻断它们

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 设备控制** 权限，才能编辑应用程序控制策略。

- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以检测设备，但不阻断它们。如果您想今后阻断设备，但需要首先检测和免除您需要的设备，那么，这一功能将很有用。

检测设备但不阻断它们，请在设备控制策略中，启用设备控制扫描，并开启仅限检测模式。更改您想要检测设备的状态“已阻断”。当策略被违反时，这将在终结点计算机上生成设备事件，但是设备将不会被阻断。

要了解有关查看设备控制事件的信息，请参见 查看设备控制事件（第59页）。

要检测设备但不阻断它们:

1. 检查哪个设备控制策略被您想要配置的计算机组所采用了。
   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **设备控制**。然后，双击您想要更改的策略。
3. 在 **设备控制策略** 对话框的 **配置** 标签页中，选择 **启用设备控制扫描**。
4. 选择 **检测但不阻断设备**。
5. 如果您尚未这样做，那么，更改您想要检测的设备的状态为“已阻断”。（要了解详情，请参见 选择要控制的设备类型。（第141页）。）
   单击 **确定**。

24.6 检测和阻断设备

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 设备控制** 权限，才能编辑应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

1. 检查哪个设备控制策略被您想要配置的计算机组所采用了。
   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **设备控制**。然后，双击您想要更改的策略。
3. 在 **设备控制策略** 对话框的 **配置** 标签页中，勾选 **启用设备控制扫描** 勾选框。
4. 取消勾选 **检测但不阻断设备** 勾选框。
5. 如果您尚未这样做，那么，更改您想要阻断的设备的状态为“已阻断”。（要了解详情，请参见 选择要控制的设备类型。（第141页）。）
   单击 **确定**。

24.7 从所有策略中免除设备

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 设备控制** 权限，才能编辑应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以从所有的策略中免除设备，包括默认的策略。该免除随后将会被添加到您创建的所有新策略中。

您可以免除设备实体（“仅限此设备”）或者，免除设备型号（“此型号的所有设备”）。不要同时设置免除型号和设备实体。如果同时定义了两者，那么，设备实体的设置将优先。

要从所有设备控制策略中免除设备:

1. 在 **查看** 菜单中，单击 **设备控制事件**。

   会出现 **设备控制 - 事件查看器** 对话框。

2. 如果您只想查看特定的事件，请在 **搜索标准** 窗格板中，设置合适的筛选项，然后，单击 **搜索** 按钮，以显示事件。

   要了解更多信息，请参见 查看设备控制事件（第59页）。

3. 选择您想从策略中免除的设备项目，然后，单击 **免除设备**。

   会出现 **免除设备** 对话框。在 **设备详情** 中，您可以看到设备类型，型号，和 ID。在 **免除详情** 的 **范围** 中，您可以看到“所有策略”字样。

   注: 如果没有您想要免除的设备的事件，例如，某终结点计算机上内建的 CD 或 DVD 驱动器，那么，请到带有此设备的计算机上，在“设备管理器”中启用此设备。（要访问“设备管理器”，请右击 **我的电脑**，单击 **管理**，然后，单击 **设备管理器**。）这将生成新的“阻断”事件，它将出现在 **设备控制 - 事件查看器** 对话框中。您然后可以按照此步骤中先前的说明来免除该设备。

4. 选择您想免除“仅限此设备”或“此型号的所有设备”。
5. 选择您想允许“完全访问”或“只读访问”该设备。
6. 在 **说明** 栏中，如果愿意，输入您的说明文字。例如，您可以说明是谁要求免除该设备的。
7. 单击 **确定**。

24.8 从单个策略中免除设备

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 设备控制** 权限，才能编辑应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域 （第11页）。

您可以从设备控制策略中免除特定的设备。

您可以免除设备实体（ “仅限此设备” ）或者，免除设备型号（ “此型号的所有设备” ）。 不要同时设置免除型号和设备实体。 如果同时定义了两者，那么，设备实体的设置将优先。

要从单个策略中免除设备:

1. 检查哪个设备控制策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略 （第24页）。
2. 在 **策略** 窗格板中，双击 **设备控制**。 然后，双击您想要更改的策略。
3. 在 **设备控制策略** 对话框的 **配置** 标签页中，单击 **添加免除项目**。

   会出现 **设备控制 - 事件查看器** 对话框。
4. 如果您只想查看特定的事件，请在 **搜索标准** 窗格板中，设置合适的筛选项，然后，单击 **搜索** 按钮，以显示事件。

   要了解更多信息，请参见 查看设备控制事件 （第59页）。
5. 选择您想从策略中免除的设备项目，然后，单击 **免除设备**。

   会出现 **免除设备** 对话框。 在 **设备详情** 中，您可以看到设备类型，型号，和 ID。 在 **免除详情** 的 **范围** 中，您可以看到 “仅限此策略” 字样。

   注: 如果没有您想要免除的设备的事件，例如，某终结点计算机上内建的 CD 或 DVD 驱动器，那么，请到带有此设备的计算机上，在 “设备管理器” 中启用此设备。 （要访问 “设备管理器” ，请右击 **我的电脑**，单击 **管理**，然后，单击 **设备管理器**。 ）这将生成新的 “阻断” 事件，它将出现在 **设备控制 - 事件查看器** 对话框中。 您然后可以按照此步骤中先前的说明来免除该设备。
6. 选择您想免除 “仅限此设备” 或 “此型号的所有设备” 。
7. 选择您想允许 “完全访问” 或 “只读访问” 该设备。
8. 在 **说明** 栏中，如果愿意，输入您的说明文字。 例如，您可以说明是谁要求免除该设备的。

9. 单击 **确定**。

24.9 查看或编辑免除设备列表

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 设备控制** 权限，才能编辑应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

要查看或编辑免除设备列表:

1. 检查哪个设备控制策略被您想要配置的计算机组所采用了。
   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **设备控制**。 然后，双击您想要更改的策略。
3. 在 **设备控制策略** 对话框的 **配置** 标签页中，选择您想要查看的免除设备类型，例如：光盘驱动器。 单击 **查看免除项目**。

   会出现 **<设备类型> 免除项目** 对话框。 如果是免除某型号的所有设备，那么，**设备 ID** 栏将是空白。

4. 如果您想要编辑免除设备列表，请按照以下说明之一做:
   - 如果您想要添加免除项目，请单击 **添加**。 要了解更多信息，请参见 从单个策略中免除设备（第144页）。
   - 如果您想要编辑免除项目，请选择该免除项目，并单击 **编辑**。 编辑 **免除设备** 对话框中相应的设置。
   - 如果您想要删除免除项目，请选择该免除项目，并单击 **删除**。

     这将从您正在编辑的策略中删除免除项目。 如果您想从其它策略中删除该设备，请在各个策略中重复此任务中的这些步骤。

25 配置 NAC 策略

25.1 关于 NAC

您可以设置网络访问控制(NAC)，这样，只有符合您设置的条件的计算机才能登录到网络中。依照默认值，计算机被允许访问网络。

Enterprise Console 与 NAC Manager 一道工作，为网络提供保护。您需要已经安装了:

- NAC Manager。您需要将它与 Enterprise Console 分开安装。
- NAC 代理。您在联网计算机上安装 NAC 代理，这样联网计算机可以与 NAC Manager 进行通讯。您可以通过 **保护计算机向导** 安装 NAC 代理。请参见 保护计算机（第42页）。

本节假定两者都已安装。

注: 如果您使用基于角色的管理，您必须具有 **策略设置 - NAC** 权限，才能查看 NAC 策略。要了解更多信息，请参见 关于角色和子领域（第11页）。

25.2 设置 NAC 服务器的 URL

如果您想要使用 NAC，那么，必须在 Enterprise Console 中指定 NAC 服务器（安装了 NAC Manager 的那台计算机）的 URL。只有这样:

- 您的计算机才能够与该 NAC Manager 通讯，并接收它们的 NAC 策略。
- 您可以在 NAC Manager 中配置 NAC 策略。

当您首次安装 Enterprise Console 时，它会试图寻找并连接该 NAC 服务器。总之，如果连接不成功，或者，如果您更改了该 NAC 服务器的路径，那么，您需要指定该 URL。

要输入或更改该 URL:

1. 在 **工具** 菜单中，选择 **配置 NAC URL**。
2. 在 **Sophos NAC URL** 对话框中，输入 NAC 服务器的 URL（如: http://server

   注: 如果安装 Sophos NAC 的是多台服务器，那么，请使用运行了应用程序本身的那台服务器的地址，而不要使用安装了数据库的那台服务器的地址。

3. 要核实 Enterprise Console 是否能通过所提供的 URL 连接到 NAC 服务器，请单击 **测试连接**。

25.3 启动 NAC Manager

NAC Manager 是用来编辑 NAC 策略的界面。

要启动 NAC Manager:

1. 单击工具栏上的 **NAC** 按钮。

   或者，在 **工具** 菜单中，选择 **管理 NAC**。

   注: 如果事先没有指定，或者，没有检测到 NAC 服务器 URL，您会被提示指定它。

2. 使用您的 Sophos NAC 用户认证资料（它由 Sophos NAC 系统管理员提供）登录。

要了解该界面的完整详情，请参见 Sophos NAC Manager 帮助文件，或 *Sophos NAC for Endpoint Security and Control NAC Manager* 指南。

25.4 什么是默认的 NAC 设置?

依照默认值，**默认的** NAC 策略会应用到已安装了 NAC 功能的计算机上。除非您已更改了“策略模式”，这意味着:

- 计算机被允许访问网络。
- NAC 运行在“仅限报告”模式中。

要了解预设的 **受管理的** 和 **未管理的** 策略的详情，请参见。什么是预设的 *NAC* 策略?（第147页）

25.5 什么是预设的 NAC 策略?

有三种预设的策略可以使用。您可以编辑各个策略中的设置，具体说明请见编辑 *NAC* 策略（第148页）。

默认

此策略默认应用到已安装了NAC功能的计算机上。计算机会被允许访问网络，除非您已经更改了该策略的设置。NAC 在“仅限报告”模式中运行。

受管理的

此策略可以用于受到 Enterprise Console 管理并且已安装了 NAC 的计算机。它的初始设置与默认策略相同。

未管理

此策略可以用于来自公司之外的计算机，它们未受 Enterprise Console 的管理，也没有安装 NAC。您的公司可以要求这样的来宾用户，连接到某个网站上，那里会有一个网页代理，在允许来宾用户的计算机访问网络之前，对照策略对它们进行评估。

25.6 编辑 NAC 策略

如果您使用基于角色的管理，您必须具有**策略设置-NAC**权限，才能编辑NAC策略。 要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以更改任何预设的 NAC 策略中的设置。 您可以在 NAC Manager 中编辑策略，更改策略模式，策略中的配置文件，或应用到策略中的网络访问模板。

要编辑 NAC 策略:

1. 在 **策略** 窗格板中，双击 **NAC**。 双击您想要更改的策略。

   NAC Manager 会启动。

2. 使用您的认证资料登录。
3. 在该策略的页面中，编辑选项。

要了解更多有关更新预设的策略的信息，请参见 *Sophos NAC Manager* 配置指南（英文）。

26 配置介入防范策略

26.1 关于介入防范

介入防范使您能够防范已知的恶意软件，以及防止未经授权的用户通过Sophos Endpoint Security and Control 用户界面，卸载或禁用 Sophos 安全软件。

注: 介入防范不是用来针对技术知识丰富的用户的。它无法防范专门瓦解操作系统的检测功能的恶意软件。.此类的软件只能通过对安全隐患和可疑行为的扫描，才能被发现。（要了解更多信息，请参见“配置防病毒和 HIPS 策略”部分。）

在您启用了介入防范，并创建了介入密码之后，终结点计算机上的 SophosAdministrator 组中不知道密码的成员，将不能够:

- 在 Sophos Endpoint Security and Control 中重新配置读写扫描或可疑行为检测设置。
- 禁用介入防范。
- 卸载 Sophos Endpoint Security and Control 组件（Sophos Anti-Virus， Sophos Client Firewall， Sophos AutoUpdate， 或 Sophos Remote Management System）。
- 卸载 Sophos SafeGuard Disk Encryption。

如果您想要使 SophosAdministrators 组成员能够执行这些任务，请向他们提供介入防范密码，以便他们能够通过介入防范的身份认证，执行这些任务。

介入防范不会影响到 SophosUser 和 SophosPowerUser 组中的成员。当介入防范启用时，他们将能够执行所有通常已经授权执行的任务，并不需要输入介入防范密码。

注: 如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 介入防范** 权限，才能配置介入防范策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

介入防范事件

当出现介入防范事件时，例如，阻止了某个未经授权的用户试图卸载某个终结点计算机上的 Sophos Anti-Virus 时，该事件会被记录到日志中，并可以从 Enterprise Console 中查看该日志记录。要了解详情，请参见 查看介入防范事件（第60页）。

介入防范事件有两种类型:

- 顺利的介入防范验证事件，显示已验证的用户的名称，以及验证的时间。
- 不成功的介入尝试事件，显示涉及的 Sophos 软件产品或组件的名称，介入尝试的时间，以及进行介入尝试的用户的详情。

26.2 开启或关闭介入防范

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 介入防范** 权限，才能配置介入防范策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

要开启或关闭介入防范:

1. 检查您想要配置的计算机组所采用了哪个介入防范策略。

   请参见 查看组采用的策略（第24页）。

2. 在 **策略** 窗格板中，双击 **介入防范**。然后，双击您想要更改的策略。

3. 在 **介入防范策略** 对话框中，勾选或取消勾选 **启用介入防范** 勾选框。

   如果您是首次启用介入防范，请单击 **密码** 框下的 **设置**。在 **介入防范密码** 对话框中，输入并确认密码。

   提示： 我们建议密码长度应该至少有 8 个字符，并且包含大小写字母和数字。

26.3 更改介入防范密码

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 介入防范** 权限，才能配置介入防范策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

要更改介入防范密码

1. 检查您想要配置的计算机组所采用了哪个介入防范策略。

   请参见 查看组采用的策略（第24页）。
2. 在 **策略** 窗格板中，双击 **介入防范**。然后，双击您想要更改的策略。
3. 在 **介入防范策略** 对话框中，单击 **密码** 文本框下的 **更改**。在 **介入防范密码** 对话框中，输入并确认新的密码。

   提示： 密码长度应该至少有 8 个字符，并且包含大小写字母和数字。

27 设置警报

27.1 关于警报

在 Enterprise Console 中有数种发送警报的方法可供使用。

- **在控制台中显示的警报。**

  如果在计算机中发现了需要关注的项目，或者出现了错误，Sophos Endpoint Security and Control 会向 Enterprise Console 发送警报。 在计算机列表中显示的警报。 要了解更多有关此类警报的信息，请参见“处置警报”部分。

  这些警报总是会被显示。 您不必设置它们。

- **在控制台中显示的事件。**

当某终结点计算机上出现应用程序控制，防火墙，数据控制，或设备控制事件时，例如，某应用程序已被防火墙阻断，该事件会被发送到 Enterprise Console，并且可以在相应的事件查看器中被查看。

- **控制台发送给您选择的收件人的警报**

  依照默认值，当计算机中检测到某个项目时，会出现桌面警报，以及记录会添加到 Windows 事件日志中。 当发生应用程序控制，数据控制，或设备控制事件时，消息会显示在计算机桌面上。

  您还可以为系统管理员设置电子邮件警报或 SNMP 警报。

本节将说明怎样设置发送给您选择的收件人的警报。

27.2 设置软件预订警报

如果您使用基于角色的管理，那么，您必须具有 **系统配置** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

Enterprise Console 会显示更新管理器在 **更新管理器** 视图的 **警报** 栏中给出的警报。 如果您预订了固定版本的软件，当该版本即将淘汰或已淘汰时，会出现警报。

如果您选择了 **当出现 Sophos 不再支持的固定版软件时，自动升级该固定版软件。**，您的预订会自动升级。

如果您没有选择自动升级，您将被指导更改您的预订。

重要: 运行不再支持的软件，将使您无法防范新出现的安全隐患。 Sophos 建议尽快更新到受支持的版本。

您还可以设置电子邮件警报，当您预订的产品的版本即将淘汰或已淘汰时，向您所选择的收件人寄送警报。

1. 在 **工具** 菜单中，选择 **配置电子邮件警报**。

   会出现 **配置电子邮件警报** 对话框。

2. 如果尚未配置 SMTP 设置，或者，如果您想要查看或更改设置，请单击 **配置**。

   在 **配置 SMTP 设置** 对话框中，按照以下说明输入详情。

   a) 在 **服务器地址** 文本框中，输入主机名或 SMTP 服务器的 IP 地址。

   b) 在 **寄件人** 文本框中，输入退回邮件和未送达报告将要寄往的地址。

   c) 单击 **测试** 测试连接情况。

3. 在 **收件人** 面板中，单击 **添加**。

   会出现 **添加新的电子邮件警报收件人** 对话框。

4. 在 **电子邮件地址** 文本框中，输入您的收件人的地址。
5. 在 **语言** 文本框中，选择寄送电子邮件警报所使用的语言。
6. 在 **预订** 窗格板中，选择您想要寄给该收件人的“更新管理器”电子邮件警报。 您可以预订两种警报:
   - 软件预订中包括很快就要在 Sophos 淘汰的产品版本。
   - 软件预订中包括已在 Sophos 淘汰的产品版本。

27.3 设置防病毒和 HIPS 电子邮件警报

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

如果组中的任何一台计算机中出现病毒，可疑行为，可能不想安装的应用程序，或错误，您可以向特定的用户寄送电子邮件警报。

重要: Mac OS X 计算机只能向一个地址寄送电子邮件警报。

1. 在 **策略** 窗格板中，双击您想要更改的防病毒和 HIPS 策略。
2. 在 **防病毒和 HIPS 策略** 对话框的 **配置防病毒和 HIPS** 面板中，单击 **消息发送**。
3. 在 **消息发送** 对话框中的 **电子邮件警报发送** 标签页中，选择 **启用电子邮件警报发送**。
4. 在 **要发送的消息** 窗格板中，选择想要针对它发送电子邮件警报的事件。

   注: **可疑行为检测**，**可疑文件检测**，以及 **广告软件和可能不想安装的应用程序检测和清除** 的设置仅应用于 Windows 2000 及以后。 **其它错误** 的设置只应用于 Windows 计算机。

5. 在 **收件人** 面板中，单击 **添加** 或 **删除** 分别添加或删除电子邮件警报的寄往地址。 单击 **重命名** 更改您所添加的电子邮件地址。

   重要: Mac OS X 计算机将只向列表中的第一个收件人发送邮件。

6. 单击 **配置 SMTP**，更改 SMTP 服务器和电子邮件警报语言的设置。

7. 在 **配置 SMTP 设置** 对话框中，按照以下说明输入详情。

   - 在 **SMTP 服务器** 文本框中，输入主机名或 SMTP 服务器的 IP 地址。 单击 **测试** 发送测试的电子邮件警报。

   - 在 **SMTP 寄件人地址** 文本框中，输入退回邮件和未送达报告将要寄往的地址。

   - 在 **SMTP 回复地址** 文本框中，您可以在文本框中，输入电子邮件警报的回复地址。 电子邮件警报是从无人照管的邮箱发出的。

     注: Linux 和 UNIX 计算机将忽略 SMTP 寄件人和回复地址，并使用地址 “root@<hostname>” 。

   - 在 **语言** 窗格板中，单击下拉箭头，然后选择寄送电子邮件警报所使用的语言。

27.4 设置防病毒和 HIPS SNMP 警报

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

如果组中的任何一台计算机中出现病毒或错误，您可以向特定的用户寄送SNMP警报。

注: 这些设置仅应用于 Windows 2000 及以后。

1. 在 **策略** 窗格板中，双击您想要更改的防病毒和 HIPS 策略。
2. 在 **防病毒和 HIPS 策略** 对话框的 **配置防病毒和 HIPS** 面板中，单击 **消息发送**。
3. 在 **消息发送** 对话框中的 **SNMP 消息发送** 标签页中，选择 **启用 SNMP 消息发送**。
4. 在 **要发送的消息** 窗格板中，选择您想要 Sophos Endpoint Security and Control 针对它发送 SNMP 消息的事件类型。
5. 在 **SNMP 陷阱目标** 文本框中，输入收件人的 IP 地址。
6. 在 **SNMP 团体名** 文本框中，输入 SNMP 团体名。

27.5 配置防病毒和 HIPS 桌面警报

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

依照默认值，桌面警报会显示在发现病毒，可疑项目，或可能不想安装的应用程序的计算机上。 您可以配置这些警报。

1. 在 **策略** 窗格板中，双击您想要更改的防病毒和 HIPS 策略。
2. 在 **防病毒和 HIPS 策略** 对话框的 **配置防病毒和 HIPS** 面板中，单击 **消息发送**。
3. 在 **消息发送** 对话框中，单击 **桌面消息发送** 标签。

   依照默认值，**启用桌面消息发送** 和 **要发送的消息** 窗格板中的所有选项都将被选择。 如果需要，可以编辑这些设置。

   注: **可疑行为检测**，**可疑文件检测**，以及 **广告软件和可能不想安装的应用程序检测** 的设置仅应用于 Windows 2000 及以后。

4. 在 **用户自定义消息** 文本框中，您可以可以输入一段消息文字，它会被添加到标准的消息文字之后。

27.6 设置应用程序控制警报

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 应用程序控制** 权限，才能配置应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

当发现受控程序时，您可以向特定的用户发送警报。

1. 在 **策略** 窗格板中，双击您想要更改的应用程序控制策略。
2. 在 **应用程序控制策略** 对话框的 **消息发送** 页中。

   消息发送 窗格板中的 **启用桌面消息发送** 勾选框，依照默认值已被勾选。 当读写扫描检测到，并阻断了未经批准的受控程序时，会有桌面消息显示给用户，告知他们该应用程序已被阻断。

3. 在 **消息** 文本框中，您可以输入一段消息文字，它会被添加到标准的桌面消息之后。

4. 如果您想要发送有关检测到的受控程序的电子邮件警报，请勾选 **启用电子邮件警报发送** 勾选框。
5. 如果您想要发送 SNMP 消息，请勾选 **启用 SNMP 消息发送** 勾选框。

   注: 您的防病毒和 HIPS 策略设置，将决定电子邮件和 SNMP 消息发送的配置和收件人。 要了解更多信息，请参见 *设置防病毒和 HIPS SNMP 警报*（第153页）。

27.7 设置数据控制警报

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 数据控制** 权限，才能配置数据控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

Enterprise Console 使用事件和消息报告，检测到的或阻断的敏感数据传输。

要了解更多有关数据控制策略和事件的信息，请参见“配置数据控制策略”部分。

当数据控制启用时，依照默认值，以下事件和消息会记录在日志文件中，或者，会被显示:

- 数据控制事件会被记录在工作站计算机上的日志文件中。
- 数据控制事件会被发送到 Enterprise Console 中，可以通过 **数据控制 - 事件查看器** 查看它们。（要打开事件查看器，请在 **查看** 菜单中，单击 **数据控制事件**。）

  注: 每个计算机每小时最多可以向 Enterprise Console 发送 50 个数据控制事件。

- 在最近七日之内，发生数据控制事件的数量超过了指定的级别的计算机，会显示在指标面板中。
- 桌面消息会显示在工作站计算机上。

您还可以配置 Enterprise Console 发送以下消息:

电子邮件警报	电子邮件消息会发送给您指定的收件人。
SNMP 消息	SNMP 消息会发送给您在“防病毒和 HIPS 策略”设置中指定的收件人。

要设置数据控制警报:

1. 请检查您想要配置的计算机组使用的是哪个数据控制策略。

   请参见 查看组采用的策略（第24页）。

2. 在 **策略** 窗格板中，双击 **数据控制**。然后，双击您想要更改的策略。

   会出现 **数据控制策略** 对话框。

3. 在 **数据控制策略** 对话框中，转到 **消息发送** 标签页。桌面消息发送依照默认值是启用的，并且 **在消息中包括匹配的规则** 已被勾选。
4. 如果您愿意，请输入消息文字，它会被添加到标准的消息文字之后，供用户确认文件传输和阻断文件传输时使用。
5. 要启用电子邮件警报，请勾选 **启用电子邮件警报** 勾选框。在 **电子邮件收件人** 栏中，输入收件人的电子邮件地址。使用分号 (;) 分隔各个地址。
6. 要启用 SNMP 消息发送，请勾选 **启用 SNMP 消息发送** 勾选框。

   电子邮件服务器和 SNMP 陷阱的设置，是通过“防病毒和 HIPS 策略” 配置的。

27.8 设置设备控制警报

如果您使用基于角色的管理，那么，:

- 您必须具备 **策略设置 - 设备控制** 权限，才能编辑应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

当检测到或已阻断受控设备时，Enterprise Console 通过事件和消息进行报告。

要了解更多有关设备控制策略和事件的信息，请参见“配置设备控制策略”部分。

当设备控制启用时，依照默认值，以下事件和消息会记录在日志文件中，或者，会被显示:

- 设备控制事件会被记录在工作站计算机上的日志文件中。
- 设备控制事件会被发送到 Enterprise Console 中，可以通过 **设备控制 - 事件查看器** 查看它们。（要打开事件查看器，请在 **查看** 菜单中，单击 **设备控制事件**。）
- 在最近七日之内，发生设备控制事件的数量超过了指定的级别的计算机，会显示在指标面板中。
- 桌面消息会显示在工作站计算机上。

您还可以配置 Enterprise Console 发送以下消息:

电子邮件警报	电子邮件消息会发送给您指定的收件人。
SNMP 消息	SNMP 消息会发送给您在“防病毒和 HIPS 策略”设置中指定的收件人。

要设置设备控制警报:

1. 检查哪个设备控制策略被您想要配置的计算机组所采用了。

   请参见 查看组采用的策略(第24页)。

2. 在 **策略** 窗格板中，双击 **设备控制**。 然后，双击您想要更改的策略。
3. 在 **设备控制策略** 对话框的 **消息发送** 标签页中，依照默认值，桌面消息发送已启用。 要进一步配置消息发送，请按照以下说明做:
   - 要为桌面消息发送输入消息文本，请在 **消息文本** 文本框中，输入将被添加到标准的消息文字之后的文字。
   - 要启用电子邮件警报，请勾选 **启用电子邮件警报** 勾选框。 在 **电子邮件收件人** 栏中，输入收件人的电子邮件地址。使用分号 (;) 分隔各个地址。
   - 要启用 *SNMP* 消息发送，请勾选 **启用 SNMP 消息发送** 勾选框。

   电子邮件服务器和 SNMP 陷阱的设置，是通过“防病毒和 HIPS 策略” 配置的。

27.9 设置网络状态电子邮件警报

如果您使用基于角色的管理，那么，您必须具有 **系统配置** 权限，才能配置网络状态电子邮件警报。 要了解更多信息，请参见 关于角色和子领域(第11页)。

您可以设置电子邮件警报，当指标面板中出现“警告”或“越过了紧要级”时，可以向您所选择的收件人寄送警报。

1. 在 **工具** 菜单中，选择 **配置电子邮件警报**。

   会出现 **配置电子邮件警报** 对话框。

2. 如果尚未配置 SMTP 设置，或者，如果您想要查看或更改设置，请单击 **配置**。 在 **配置 SMTP 设置** 对话框中，按照以下说明输入详情。
   a) 在 **服务器地址** 文本框中，输入主机名或 SMTP 服务器的 IP 地址。
   b) 在 **寄件人** 文本框中，输入退回邮件和未送达报告将要寄往的地址。
   c) 单击 **测试** 测试连接情况。
3. 在 **收件人** 面板中，单击 **添加**。

   会出现 **添加新的电子邮件警报收件人** 对话框。
4. 在 **电子邮件地址** 文本框中，输入您的收件人的地址。
5. 在 **语言** 文本框中，选择寄送电子邮件警报所使用的语言。
6. 在 **预订** 窗格板中，选择您想要寄给该收件人的“越过了警告级”和“越过了紧要级”电子邮件警报。

27.10 设置 Active Directory 同步化电子邮件警报

如果您使用基于角色的管理，那么，您必须具有 **系统配置** 权限，才能配置 Active Directory 同步化电子邮件警报。 要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以设置电子邮件警报，以便在与 Active Directory 同步化过程中，找到新的计算机和组时，可以向您所选择的收件人寄送警报。 如果您选择了自动保护已同步化的组中的计算机，那么，您还可以设置在自动保护失败时，发出警报。

1. 在 **工具** 菜单中，选择 **配置电子邮件警报**。

   会出现 **配置电子邮件警报** 对话框。
2. 如果尚未配置 SMTP 设置，或者，如果您想要查看或更改设置，请单击 **配置**。

   在 **配置 SMTP 设置** 对话框中，按照以下说明输入详情。
   a) 在 **服务器地址** 文本框中，输入主机名或 SMTP 服务器的 IP 地址。
   b) 在 **寄件人** 文本框中，输入退回邮件和未送达报告将要寄往的地址。
   c) 单击 **测试** 测试连接情况。
3. 在 **收件人** 面板中，单击 **添加**。

   会出现 **添加新的电子邮件警报收件人** 对话框。
4. 在 **电子邮件地址** 文本框中，输入您的收件人的地址。

5. 在 **语言** 文本框中，选择寄送电子邮件警报所使用的语言。
6. 在 **预订** 窗格板中，选择您想要寄给该收件人的“Active Directory 同步化”电子邮件警报。

   “Active Directory 同步化” 电子邮件警报:

   - 找到的新组
   - 找到的新计算机
   - 自动保护计算机失败

27.11 配置 Windows 事件日志记录

如果您使用基于角色的管理，那么，

- 您必须具备 **策略设置 - 防病毒和 HIPS** 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参见 关于角色和子领域（第11页）。

依照默认值，当检测到或清除了病毒或间谍软件，检测到可疑行为，或检测到或清除了广告软件或可能不想安装的应用程序时，Sophos Endpoint Security and Control 会将警报添加到 Windows 2000 或以后的事件日志记录中。

要编辑这些设置:

1. 在 **策略** 窗格板中，双击您想要更改的防病毒和 HIPS 策略。
2. 在 **防病毒和 HIPS 策略** 对话框的 **配置防病毒和 HIPS** 面板中，单击 **消息发送**。
3. 在 **消息发送** 对话框的 **事件日志** 标签页中。

   依照默认值，事件日志记录已启用。如果需要，可以编辑设置。

   扫描错误 中包括 Sophos Endpoint Security and Control 被拒绝访问试图扫描的项目的情况。

28 生成报告

28.1 关于报告

报告可以提供有关您的网络安全状态的各个方面的文字和图形的信息。

报告是通过 **报告管理器** 提供的。使用 **报告管理器**，您可以基于现成的模板迅速创建报告，更改现有的报告的配置，以及计划安排报告按照固定的频率运

行，并将报告以电子邮件附件的方式发送给您选择的收件人。您还可以打印报告，以及用多种格式导出报告。

Sophos提供了一系列您可以现成使用的，或者，可以按照您的需要修改它们配置的各种报告。这些报告的种类有:

- 警报和事件历史
- 警报摘要
- 按照项目名称名称排序的警报和事件
- 按照时间排序的警报和事件
- 按照路径排序的警报和事件
- 终结点计算机策略非遵照
- 按照用户排序的事件
- 受管理的终结点保护
- 更新层级

报告和基于角色的管理

如果您使用基于角色的管理，您必须具有 **报告配置** 权限，才能创建，编辑，或删除报告。如果您没有这样的权限，那么，您只能运行报告。要了解更多有关基于角色的管理的信息，请参见 关于角色和子领域（第11页）。

报告只能包含来自活动自领域中的数据。您不能在子领域之间共享报告。默认的报告不能从**默认的**子领域复制到您创建的新的子领域。

当您删除某个子领域时，该子领域中所有报告都会被删除。

28.2 创建新报告

如果您使用基于角色的管理，那么，您必须具有 **报告配置** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

要创建报告:

1. 单击工具栏中的 **报告** 图标。
2. 在 **报告管理器** 对话框中，单击 **创建**。

3. 在 **创建新报告** 对话框中，选择某个报告模板，并单击 **确定**。

   会一个向导根据您选择的模板，指导您完成创建报告。

   如果您不想使用向导，请在 **创建新报告** 对话框中，取消勾选 **使用向导创建报告** 勾选框。 然后，您可以在报告属性对话框中配置您的新建报告。 要了解更多的信息，请参见有关配置相关报告的主题。

28.3 配置警报和事件历史报告

如果您使用基于角色的管理，那么，您必须具有 **报告配置** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

警报和事件历史 报告显示每个特定的报告期间的警报和事件。

1. 单击工具栏中的 **报告** 图标。
2. 在 **报告管理器** 对话框中，选择 **警报和事件历史**，并单击 **属性**。
3. 在 **警报和事件历史属性** 对话框的 **配置** 标签页，设置您想要的选项。

   a) 在 **报告详情** 窗格板中，如果您愿意，可以编辑报告的名称和描述。

   b) 在 **报告发送期间** 窗格板的 **时间跨度** 文本框中，单击下拉箭头，并选择时间期间。

      您既可以选择一个固定的时间，如：**上个月**，也可以选择 **自定义** 并在 **始于** 和 **止于** 框中指定您自己的时间跨度。

   c) 在 **报告路径** 窗格板中，单击 **计算机组** 或 **单个计算机**。 然后，单击下拉箭头，指定组或计算机的名称。

   d) 在 **要包括的警报和事件类型** 窗格板中，选择您想要包括在报告中的警报和事件类型。

      依照默认值，报告会显示所有警报和事件类型。

      或者，您可以配置报告，仅显示报告了特定的警报或事件的路径。 要指定单个的警报或事件，请单击 **高级**，并单击列表中的警报或事件名称。要指定多个警报或事件，使用通配符，在文本框中输入安全隐患名称。使用 ? 替代名称中的单个字符，以及使用 * 替代名称中的字符串。 例如：使用 W32/* 将指定名称以 W32/ 开头的所有病毒。

4. 在 **显示选项** 标签页中，选择您想怎样排序警报和事件。

   依照默认值，警报和事件详情是按照 **警报和事件名称** 排序的。 不过，报告也可以按照 **计算机名称**，计算机的 **组名**，或者 **日期和时间**。

5. 在 **计划** 标签中，如果您想要定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人，请选择**计划此报告**。输入起始日期和时间，以及生成报告的频率，指定输出文件的格式和语言，并输入报告收件人的电子邮件地址。

28.4 配置警报摘要报告

如果您使用基于角色的管理，那么，您必须具有 **报告配置** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

警报摘要报告提供有关您的网络的状态和总体健康状况的统计数据。

1. 单击工具栏中的 **报告** 图标。
2. 在 **报告管理器** 对话框中，选择 **警报摘要**，并单击 **属性**。
3. 在 **警报摘要属性** 对话框的 **配置** 标签页中，设置您想要的选项。
   a) 在 **报告详情** 窗格板中，如果您愿意，可以编辑报告的名称和描述。
   b) 在 **报告发送期间** 窗格板的 **时间跨度** 文本框中，单击下拉箭头，并选择时间期间。

      您既可以选择一个固定的时间，如：**上个月**，也可以选择 **自定义** 并在 **始于** 和 **止于** 框中指定您自己的时间跨度。
4. 在**显示选项**标签页中的**显示结果按照**下，指定测试非遵照的时间段，如：每小时或每天，单击下拉箭头，并选择时间段。
5. 在 **计划** 标签中，如果您想要定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人，请选择**计划此报告**。输入起始日期和时间，以及生成报告的频率，指定输出文件的格式和语言，并输入报告收件人的电子邮件地址。

28.5 配置按照项目名称给出警报和事件的报告

如果您使用基于角色的管理，那么，您必须具有 **报告配置** 权限，才能执行此任务。要了解更多信息，请参见 关于角色和子领域（第11页）。

按照项目名称给出警报和事件的报告，提供在所选择的报告期间，所有计算机上的所有警报和事件的统计摘要，以项目名称归类。

要配置报告:

1. 单击工具栏中的 **报告** 图标。
2. 在 **报告管理器** 对话框中，选择 **按照项目名称给出警报和事件**，并单击 **属性**。

3. 在 **按照项目名称给出警报和事件属性** 对话框的 **配置** 标签页中，设置您想要的选项。

   a) 在 **报告详情** 窗格板中，如果您愿意，可以编辑报告的名称和描述。

   b) 在 **报告发送期间** 窗格板的 **时间跨度** 文本框中，单击下拉箭头，并选择时间期间。

      您既可以选择一个固定的时间，如：**上个月**，也可以选择 **自定义** 并在 **始于** 和 **止于** 框中指定您自己的时间跨度。

   c) 在 **报告路径** 窗格板中，单击 **计算机组** 或 **单个计算机**。 然后，单击下拉箭头，指定组或计算机的名称。

   d) 在 **要包括的警报和事件类型** 窗格板中，选择您想要包括在报告中的警报和事件类型。

      依照默认值，报告会显示所有警报和事件类型。

4. 在 **显示选项** 标签页的 **显示** 下，选择您想要在报告中显示的警报和事件。

   依照默认值，报告会显示所有的警报和事件，以及每个计算机合组中出现警报的次数。

   您还可以配置报告仅显示:

   - 前 n 个警报和事件（这里的 n 是您指定的数值），或者
   - 发生率不低于 m 的警报和事件（这里的 m 是您指定的数值）。

5. 在 **排序依据** 下，选择您想按照项目数还是警报和事件名称排序。

   依照默认值，报告列示的警报和事件，是按照警报数发生数，降序排列的。

6. 在 **计划** 标签中，如果您想要定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人，请选择 **计划此报告**。 输入起始日期和时间，以及生成报告的频率，指定输出文件的格式和语言，并输入报告收件人的电子邮件地址。

28.6 配置按照时间给出警报和事件的报告

如果您使用基于角色的管理，那么，您必须具有 **报告配置** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

按照时间给出警报和事件 的报告显示在特定的时间段出现的警报和事件的摘要。

1. 单击工具栏中的 **报告** 图标。
2. 在 **报告管理器** 对话框中，选择 **按照时间给出警报和事件**，并单击 **属性**。

3. 在 **按照时间给出警报和事件属性** 对话框的 **配置** 标签中，设置您想要的选项。

    a) 在 **报告详情** 窗格板中，如果您愿意，可以编辑报告的名称和描述。

    b) 在 **报告发送期间** 窗格板的 **时间跨度** 文本框中，单击下拉箭头，并选择时间期间。

    您既可以选择一个固定的时间，如：**上个月**，也可以选择 **自定义** 并在 **始于** 和 **止于** 框中指定您自己的时间跨度。

    c) 在 **报告路径** 窗格板中，单击 **计算机组** 或 **单个计算机**。 然后，单击下拉箭头，指定组或计算机的名称。

    d) 在 **要包括的警报和事件类型** 窗格板中，选择您想要包括在报告中的警报和事件类型。

    依照默认值，报告会显示所有警报和事件类型。

    或者，您可以配置报告，仅显示报告了特定的警报或事件的路径。 要指定单个的警报或事件，请单击 **高级**，并单击列表中的警报或事件名称。 要指定多个警报或事件，使用通配符，在文本框中输入安全隐患名称。 使用 ? 替代名称中的单个字符，以及使用 * 替代名称中的字符串。 例如：使用 W32/* 将指定名称以 W32/ 开头的所有病毒。

4. 在 **显示选项** 标签页中，指定测试警报和事件率的时间段，如：每小时或每天，单击下拉箭头，并选择时间段。

5. 在 **计划** 标签中，如果您想要定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人，请选择 **计划此报告**。 输入起始日期和时间，以及生成报告的频率，指定输出文件的格式和语言，并输入报告收件人的电子邮件地址。

28.7 配置按照路径排序的警报和事件的报告

如果您使用基于角色的管理，那么，您必须具有 **报告配置** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

按照路径给出警报和事件的报告，提供在所选择的报告期间，所有计算机上的所有警报的统计摘要，以路径归类。

1. 单击工具栏中的 **报告** 图标。
2. 在 **报告管理器** 对话框中，选择 **按照路径给出警报和事件**，并单击 **属性**。

3. 在 **按照路径给出警报和事件属性** 对话框的 **配置** 标签中，设置您想要的选项。

   a) 在 **报告详情** 窗格板中，如果您愿意，可以编辑报告的名称和描述。

   b) 在 **报告发送期间** 窗格板的 **时间跨度** 文本框中，单击下拉箭头，并选择时间期间。

      您既可以选择一个固定的时间，如：**上个月**，也可以选择 **自定义** 并在 **始于** 和 **止于** 框中指定您自己的时间跨度。

   c) 在 **报告路径** 窗格板中，单击 **计算机** 以显示每个计算机上的警报，或单击 **组** 以显示计算机上的各个组的警报。

   d) 在 **要包括的警报和事件类型** 窗格板中，选择您想要包括在报告中的警报和事件类型。

      依照默认值，报告会显示所有警报和事件类型。

      或者，您可以配置报告，仅显示报告了特定的警报或事件的路径。 要指定单个的警报或事件，请单击 **高级**，并单击列表中的警报或事件名称。要指定多个警报或事件，使用通配符，在文本框中输入安全隐患名称。使用 ? 替代名称中的单个字符，以及使用 * 替代名称中的字符串。例如：使用 W32/* 将指定名称以 W32/ 开头的所有病毒。

4. 在 **显示选项** 标签页的 **显示** 下，选择您想要在报告中显示的警报。

   依照默认值，报告会显示所有的计算机和组，以及每个计算机合组中出现警报的次数。 您可以配置报告，仅显示：

   - 前 *n* 个记录了最多次警报和事件的路径（这里的 *n* 是您指定的数值），或者
   - 不少于 *m* 个警报和事件以上的路径（这里的 *m* 是您指定的数值）。

5. 在 **排序依据** 下，选择您想按照检测到的项目数还是警报名称排序。

   依照默认值，报告列示的路径，是按照每一路径记录的警报和事件数，从高到低排列的。 如果您想要它们以字母为序，按路径名称排列，请选择 **路径**。

6. 在 **计划** 标签中，如果您想要定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人，请选择 **计划此报告**。 输入起始日期和时间，以及生成报告的频率，指定输出文件的格式和语言，并输入报告收件人的电子邮件地址。

28.8 配置终结点计算机策略非遵照报告

如果您使用基于角色的管理，那么，您必须具有 **报告配置** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

终结点计算机策略非遵照报告，显示在指定的时间段中，没有遵照所在的组的策略的计算机的百分比或数量。

1. 单击工具栏中的 **报告** 图标。
2. 在 **报告管理器** 对话框中，选择 **终结点计算机策略非遵照**，并单击 **属性**。
3. 在 **终结点计算机策略非遵照属性** 对话框的 **配置** 标签页中，设置您想要的选项。
   a) 在 **报告详情** 窗格板中，如果您愿意，可以编辑报告的名称和描述。
   b) 在 **报告发送期间** 窗格板的 **时间跨度** 文本框中，单击下拉箭头，并选择时间期间。

      您既可以选择一个固定的时间，如: **上个月**，也可以选择 **自定义** 并在 **始于** 和 **止于** 框中指定您自己的时间跨度。
   c) 在 **显示** 窗格板中，选择您想要在报告中显示的策略。依照默认值，只有**防病毒和 HIPS** 策略被选择。
4. 在 **显示选项** 标签页中的 **显示结果按照** 下，指定测试非遵照的时间段，如: 每小时或每天，单击下拉箭头，并选择时间段。
5. 在 **显示结果为** 下，选择您想要以百分比还是数字显示结果。
6. 在 **计划** 标签中，如果您想要定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人，请选择 **计划此报告**。 输入起始日期和时间，以及生成报告的频率，指定输出文件的格式和语言，并输入报告收件人的电子邮件地址。

28.9 配置每个用户的事件的报告

如果您使用基于角色的管理，那么，您必须具有 **报告配置** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

每个用户的事件的报告，显示应用程序控制（包括被阻断的网站），防火墙，数据控制，以及设备控制等事件，并按照用户归类。

1. 单击工具栏中的 **报告** 图标。
2. 在 **报告管理器** 对话框中，选择 **每个用户的事件**，并单击 **属性**。

3. 在 **每个用户的事件属性** 对话框的 **配置** 标签页中，设置您想要的选项。
   a) 在 **报告详情** 窗格板中，如果您愿意，可以编辑报告的名称和描述。
   b) 在 **报告发送期间** 窗格板的 **时间跨度** 文本框中，单击下拉箭头，并选择时间期间。

      您既可以选择一个固定的时间，如：**上个月**，也可以选择 **自定义** 并在 **始于** 和 **止于** 框中指定您自己的时间跨度。
   c) 在 **要包括的事件类型** 下，选择您想要显示事件的功能。
4. 在 **显示选项** 标签页的 **显示** 下，选择您想要在报告中显示的用户。

   依照默认值，报告会显示所有用户，以及每个用户的事件数量。您可以配置报告，仅显示:
   - 前 *n* 个记录了最多次事件的用户（这里的 *n* 是您指定的数值），或者
   - 不少于 *m* 个事件以上的用户（这里的 *m* 是您指定的数值）。
5. 在 **排序依据** 下，选择您想要按照发生的事件数还是名称排序用户。

   依照默认值，报告列示的用户，是按照每个用户发生的事件数，从高到低排列的。如果您想要它们以字母为序，按用户名称排列，请选择 **用户**。
6. 在 **计划** 标签中，如果您想要定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人，请选择 **计划此报告**。输入起始日期和时间，以及生成报告的频率，指定输出文件的格式和语言，并输入报告收件人的电子邮件地址。

28.10 配置受管理的终结点保护保护

如果您使用基于角色的管理，那么，您必须具有 **报告配置** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

受管理的终结点保护 的报告，显示在指定的时间段中，受到保护的计算机的百分比或数量。

1. 单击工具栏中的 **报告** 图标。
2. 在 **报告管理器** 对话框中，选择 **受管理的终结点保护**，并单击 **属性**。

3. 在 **受管理的终结点保护属性** 对话框的 **配置** 标签页中，设置您想要的选项。
   a) 在 **报告识别** 窗格板中，如果您愿意，可以编辑报告的名称和描述。
   b) 在 **报告发送期间** 窗格板的 **时间跨度** 文本框中，单击下拉箭头，并选择时间期间。

      您既可以选择一个固定的时间，如：**上个月**，也可以选择 **自定义** 并在 **始于** 和 **止于** 框中指定您自己的时间跨度。
   c) 在 **显示** 窗格板中，选择您想要在报告中显示的功能。
4. 在 **显示选项** 标签页中的 **显示结果按照** 下，指定测试非遵照的时间段，如：每小时或每天，单击下拉箭头，并选择时间段。
5. 在 **显示结果为** 下，选择您想要以百分比还是数字显示结果。
6. 在 **计划** 标签中，如果您想要定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人，请选择 **计划此报告**。输入起始日期和时间，以及生成报告的频率，指定输出文件的格式和语言，并输入报告收件人的电子邮件地址。

28.11 更新层级报告

更新层级 报告显示您的网络中的更新管理器，它们维护的更新共享，以及从这些共享进行更新的计算机。

您不能配置 **更新层级** 报告。 您可以按照 运行报告（第169页） 中的说明运行报告。

28.12 计划报告

如果您使用基于角色的管理，那么，您必须具有 **报告配置** 权限，才能执行此任务。 要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以计划安排定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人。

1. 单击工具栏中的 **报告** 图标。
2. 在 **报告管理器** 对话中，选择您想要计划的报告，并单击 **计划**。
3. 在出现的对话框的 **计划** 标签中，选择 **计划安排此报告**。
4. 输入开始日期和时间，以及生成报告的频率。
5. 指定输出的文件的格式和语言。
6. 输入报告收件人的电子邮件地址。

28.13 运行报告

1. 单击工具栏中的 **报告** 图标。
2. 在 **报告管理器** 对话框中，选择您想要运行的报告，并单击 **运行**。

   显示报告的 **报告发送** 窗口会出现。

您可以更改报告的页面设置，并打印报告或导出报告到文件中。

28.14 查看图表形式的报告

有些报告可以同时以表的形式和图的形式查看。如果是这种情况，在出现在报告中的 **报告发送** 窗中，您将看到两个标签页，**表** 和 **图**。

1. 单击工具栏中的 **报告** 图标。
2. 在 **报告管理器** 对话框中，选择您想要运行的报告，如：**按照每个路径提供警报和事件**，然后，单击 **运行**。

   显示报告的 **报告发送** 窗口会出现。

3. 查看图表形式的报告，请转到相应的标签页。

28.15 打印报告

要打印报告，请单击报告顶端，工具栏上的 **打印** 图标。



28.16 将报告导出到文件

要将报告导出到文件:

1. 单击单击报告顶端，工具栏中的 **导出** 图标。

2. 在 **导出报告** 对话框中，选择您想要将报告导出的文档或电子报表类型。

   选项为：

   - PDF (Acrobat)
   - HTML
   - Microsoft Excel
   - Microsoft Word
   - Rich Text Format (RTF)
   - 逗号分隔值格式(CSV)
   - XML

3. 单击 **文件名** 浏览按钮选择路径。然后，输入文件名。单击 **确定**。

28.17 更改报告的页面格式

您可以更改报告的页面格式。比如，您可以横向（宽页）的格式呈现报告。

1. 单击单击报告顶端，工具栏中的页面格式图标。

2. 在 **页面设置** 对话框中，指定页面大小，打印方向和页边距等。单击 **确定**。

   报告将会按照页面设置的格式呈现。

当您打印或导出报告时，也会使用该页面设置。

29 从 Enterprise Console 复制和打印数据

29.1 从计算机列表复制数据

您可以复制在计算机列表的 **终结点** 视图中中显示的数据，到“剪贴板”中，然后，可以将数据粘贴到“制表符分隔”格式的文档中。

1. 在 **终结点** 视图的 **组** 窗格板中，选择您想要复制数据的计算机组。
2. 在 **查看** 下拉列表中，选择您想要显示的计算机，例如，**有潜在问题的计算机**。
3. 如果该组含有子组，请选择您想显示的计算机是 **仅在这一级** 或在 **在这一级，及以下级**。
4. 在计算机列表中，在与您想要显示的内容相关的标签页中，例如，**防病毒详情**。

5. 单击计算机列表以激活它。
6. 在 **编辑** 菜单中，单击 **复制** 将数据复制到“剪贴板”中。

29.2 从计算机列表打印数据

您可以在 **终结点** 视图中打印显示在计算机列表中的信息。

1. 在 **终结点** 视图的 **组** 窗格板中，选择您想要打印数据的计算机组。
2. 在 **查看** 下拉列表中，选择您想要显示的计算机，例如，**有潜在问题的计算机**。
3. 如果该组含有子组，请选择您想显示的计算机是 **仅在这一级** 或在 **在这一级，及以下级**。
4. 在计算机列表中，在与您想要显示的内容相关的标签页中，例如，**防病毒详情**。
5. 单击计算机列表以激活它。
6. 在 **文件** 菜单中，单击 **打印**。

29.3 复制计算机详情

您可以从 **计算机详情** 对话框中复制信息到“剪贴板”中，然后，将它们粘贴到其它文档中。这些信息包括：计算机名称，计算机的操作系统，安装在计算机上的安全软件的版本，任何尚未处理的警报和错误，更新状态，等等。

1. 在 **终结点** 视图的计算机列表中，双击您想要复制数据的计算机。
2. 在 **计算机详情** 对话框中，单击 **复制**，复制数据到“剪贴板”中。

29.4 打印计算机详情

您可以从 **计算机详情** 对话框中打印信息。 这些信息包括：计算机名称，计算机的操作系统，安装在计算机上的安全软件的版本，任何尚未处理的警报和错误，更新状态，等等。

1. 在 **终结点** 视图的计算机列表中，双击您想要打印的计算机。
2. 在 **计算机详情** 对话框中，单击 **打印**。

30 别的用户怎样使用 Enterprise Console？

Sophos Full Administrators 组的成员具备完全访问 Enterprise Console 的权限。

您可以允许别的用户使用 Enterprise Console。要打开 Enterprise Console，用户必须：

- 是 Sophos Console Administrators 组中的成员。
- 被指派给至少一个 Enterprise Console 角色。
- 被指派给至少一个 Enterprise Console 子领域。

如果您想要指派某个用户给 Sophos Console Administrators 组，请使用 Windows 工具将该用户添加到组中。

要指派某个用户给某个 Enterprise Console 角色或子领域，请在 **工具** 菜单中，单击 **管理角色和子领域**。要了解更多有关角色和子领域的信息，请参见 关于角色和子领域（第11页）。

要使用远程或附加的 Enterprise Console，用户必须：

- 是 Enterprise Console Management Server 所安装的那台服务器上的 Sophos Console Administrators 组中的成员。
- 是 Enterprise Console Management Server 所安装的那台服务器上的 Distributed COM Users 组中的成员。（Distributed COM Users 组位于Active Directory Users and Computers 工具的 Builtin 容器中）。
- 被指派给至少一个 Enterprise Console 角色。
- 被指派给至少一个 Enterprise Console 子领域。
- 是 Enterprise Console 数据库所在的服务器上的 Sophos DB Users 组中的成员，以便能够运行报告。

31 开启或关闭发送报告至 Sophos

如果您使用基于角色的管理，您必须具备 **系统配置** 权限，才能开启或关闭发送报告至 Sophos。 要了解更多信息，请参见 关于角色和子领域（第11页）。

您可以选择允许 Sophos Enterprise Console 每周向 Sophos 报告已管理的计算机的数量，以及有关操作系统类型和版本，所使用的 Sophos 产品的信息。 Sophos 将利用这些信息来提供更好的技术支持服务，以及进一步了解客户使用 Sophos 产品的情况。 任何向 Sophos 报告的有关您的计算机的信息，都不会确定个人身份，以及确定具体的计算机。 Sophos 不会利用向 Sophos 报告的信息来确定您的公司，除非您向我们提供了您的 Sophos 下载用户名和／或电子邮件地址。

依照默认值，发送报告至 Sophos 是启用的。 在安装或更新控制台时，您有机会在 Sophos Enterprise Console 安装向导中，选择禁用发送报告至 Sophos 选项。

在安装之后，如果您想要开启或关闭向 Sophos 发送报告，请按照以下说明做：

1. 在 **工具** 菜单中，单击 **发送报告至 Sophos**。
2. 在 **发送报告至 Sophos** 对话框中，您可以启用或禁用发送报告。
   - 如果您想要发送报告至 *Sophos*， 请阅读协议，并选择 **我同意** 勾选框，如果您同意协议中的条款。
   - 如果您想禁用发送报告至 *Sophos*， 请取消勾选 **我同意** 勾选框。

   如果您想要启用 Sophos 客户支持可以直接与您联系，如：出现操作系统或版本问题时，请输入您的 Sophos 下载用户名和／或电子邮件地址。

   如果您乐于启用发送报告，但是想要以匿名方式进行，那么，您不必提供用户名或电子邮件地址。

32 排疑解难

32.1 计算机没有运行读写扫描

如果有计算机没有运行读写扫描:

1. 请检查这些计算机使用的防病毒和 HIPS 策略。

   要了解详情，请参见 查看组采用的策略（第24页）。
2. 请确保已在该策略中启用了读写扫描，并且这些计算机已遵照此策略。

   要了解详情，请参见 开启或关闭读写扫描（第91页） 和 使计算机采用组策略（第29页）。

32.2 防火墙已禁用

如果有计算机上的防火墙已禁用:

1. 请检查这些防火墙使用的是哪个防火墙策略。

   要了解详情，请参见 查看组采用的策略（第24页）。
2. 请确保已在该策略中启用了防火墙，并且这些计算机已遵照此策略。

   要了解详情，请参见 临时禁用防火墙（第117页） 和 使计算机采用组策略（第29页）。

32.3 防火墙未安装

注: 如果您使用基于角色的管理，那么，您必须具备 **计算机搜索，保护和组** 权限，才能安装防火墙。 要了解更多信息，请参见 关于角色和子领域（第11页）。

在您要将防火墙安装到终结点计算机上之前，请检查:

- 您的用户授权使用许可协议中是否包含防火墙。
- 计算机是否运行的是 Windows 2000 或以后的操作系统。

注: 您无法在运行服务器操作系统，或者运行 Windows Vista Starter 的计算机上安装防火墙。

如果您想要在计算机上安装防火墙:

1. 请选择该计算机，单击鼠标右键，并选择 **保护计算机**。

   会出现 **保护计算机向导**。 单击 **下一步**。

2. 当提示选择功能时，请选择 **防火墙**。 结束向导。

如果问题继续存在，请联系 Sophos 技术支持。

32.4 具有未处置的警报的计算机

- 如果有计算机感染了病毒，或者安装了您不想安装的应用程序，请参见 立即清除计算机 （第54页）。
- 如果在计算机上检测到了您想要的广告软件或其它可能不想安装的应用程序，请参见 批准广告软件和可能不想安装的应用程序 （第84页）。
- 如果有未及时更新的计算机，要获得有关诊断和解决问题的帮助，请参见 更新未及时更新的计算机 （第63页）。

注: 如果您不在需要显示警报，您可以清除它。 选择出现警报的计算机，右击并选择 **处置警报和错误**。 您必须具备 **调整-清除** 权限，才能确认已知（清空）警报和错误。

32.5 未受控制台管理的计算机

Windows，Mac，Linux，和 UNIX 计算机都应该被 Enterprise Console 管理，这样它们都可以被及时更新和监控。

注: Enterprise Console 不会自动显示和管理新加入到网络中的计算机，除非您使用了 Active Directory 同步化（请参见 关于与 *Active Directory* 同步化 （第33页））。 单击工具栏中的 **查找新计算机** 图标，可以搜索新加入到网络中的计算机，并可以将它们放置到 **未指派** 组中。

如果某计算机没有被管理，有关它的详情，在 **状态** 标签页中会被灰白显示。

要开始管理未受管理的计算机:

1. 在 **视图** 下拉列表中，选择 **未管理的计算机**。
2. 选择列示出的任何计算机。 右击并选择 **保护计算机**，安装被管理的 Sophos Endpoint Security and Control 版本。
3. 如果有任何计算机，Enterprise Console 无法为其自动安装 Sophos Endpoint Security and Control，请进行 手动安装。

   要了解详情，请参见 *Sophos Endpoint Security and Control* 高级安装指南。

32.6 无法保护在“未指派”组中的计算机。

未指派组只用于放置尚未属于任何您创建的组的计算机，策略不能应用到此组中。 直到将计算机放置到您创建的组中后，您才能保护它们。

32.7 Sophos Endpoint Security and Control 安装失败

如果 **保护计算机向导** 在计算机上安装 Sophos Endpoint Security and Control 失败，可能会是因为:

- Enterprise Console 不知道在计算机上运行的是哪个操作系统。 这可能是因为在查找计算机时，您没有以“域名\用户”的格式输入用户名。
- 自动安装不能该操作系统的计算机上进行。 执行手动安装。 要了解操作指导，请参见 Sophos Endpoint Security and Control 高级安装指南。
- 计算机上正在运行防火墙。
- 在 Windows XP 计算机上的“简单文件共享”没有关闭。
- 在 Windows Vista 计算机，“简单文件共享”选项没有关闭。
- 计算机上的操作系统不支持您选择安装的功能。

如果 Compliance Agent 的安装失败，或者，在安装过程中出现错误，您可以查看 Compliance Agent 安装日志文件。 该日志文件在 %tmp% 文件夹中。

要了解 Sophos Endpoint Security and Control 功能的系统要求的完整列表，请参见 Sophos 网站上的系统要求 (*http://cn.sophos.com/products/all-sysreqs.html*)。

32.8 计算机未被更新

要获得有关诊断和解决问题的帮助，请参见 更新未及时更新的计算机（第63页）。

32.9 防病毒设置在 Mac 计算机上不起作用

有些防病毒设置不能应用于 Mac 计算机。 在这种情况下，在设置的页面中会出现警告文字。

您可以通过 Sophos Update Manager 更改 Mac 计算机上的防病毒设置，Sophos Update Manager 是随 Sophos Anti-Virus for Mac 提供的实用工具程序。 要开启 Sophos Update Manager，在 Mac 计算机的 **Finder** 窗口中，浏览找到 Sophos Anti-Virus:ESOSX 文件夹。 双击 **Sophos Update Manager**。 要了解更多详情，请参见 Sophos Update Manager 帮助文件。

32.10 防病毒设置在 Linux 或 UNIX 计算机上不起作用

某些防病毒设置无法被应用到 Linux 或 UNIX 计算机上。 在这种情况下，在设置的页面中会出现警告文字。

您可以按照 **Sophos Anti-Virus for Linux 用户手册**（英文）中的说明，使用 **savconfig** 和 *savscan* 命令，更改 Linux 计算机上的防病毒设置。 您可以按照 **Sophos Anti-Virus for UNIX 用户手册**（英文）中的说明，使用 *savscan* 命令，更改 UNIX 计算机上的防病毒设置。

32.11 未遵照策略的 Linux 或 UNIX 计算机

如果您在CID中使用的是联合配置文件，并且该文件中的配置值与策略冲突，那么，计算机会显示为“未遵照策略”。

选择 **遵照策略** 选项只会使计算机暂时与策略一致，直到重新应用基于CID的配置为止。

要解决这个问题，请查看联合配置文件，并且在可能的情况下，用基于控制台的配置替换它。

32.12 读写扫描设置不起作用

对 Windows 95 和 Windows 98 计算机而言，在读写扫描设置页面更改某些设置，将不会起作用。 在相应的页面中会出现警告标志。

在这些情况中，您在计划扫描设置页面中所做的更改，会同时应用到计划和读写扫描中。 这是因为早期的 Windows 版本的 Sophos Anti-Virus 的设计。

32.13 Windows 2000 或以后的计算机上出现意想之外的新扫描

如果在 Windows 2000 或以后的计算机上查看本地的 Sophos Endpoint Security and Control，您可能会看到有新的“可用扫描”列示出来，即使用户并没有创建新的扫描。

这个新扫描实际上是您从控制台中设置的计划扫描。您不应该删除它。

32.14 连接和超时问题

如果 Enterprise Console 和联网计算机之间的通讯变慢，或者计算机不响应，则可能有连接问题。

请查看 Sophos 网络通讯报告，该报告提供计算机和 Enterprise Console 之间的通讯现状的概览。要查看该报告，请到出现问题的计算机中。在任务栏中，单击 **开始** 按钮，选择 **所有程序| Sophos| Sophos Endpoint Security and Control**，然后，单击 **查看 Sophos 网络通讯报告**。

报告会显示可能出现问题的地方，如果已经检测到了问题，则会提供解决措施。

32.15 没有检测到广告软件和可能不想安装的应用程序(PUA)

如果没有检测到广告软件和其它可能不想安装的应用程序 (PUA)，那么，您应该检查:

- 检测是否已启用。请参见 扫描广告软件和可能不想安装的应用程序（第83页）。
- 应用程序所运行的计算机运行的是 Windows 2000 或以后的操作系统。

32.16 部分检测到项目

Sophos Endpoint Security and Control 可能会报告该项目（例如，特洛伊木马或可能不想安装的应用程序）为“部分检测到”。这说明 Sophos Anti-Virus 没有找到该应用程序的所有组件。

要找到其它组件，您需要对被涉及的计算机做完整系统扫描。在运行 Windows 2000 或以后操作系统的计算机上，您可以通过选择计算机，右击并选择 **完整系统扫描** 来实现。您也可以通过设置针对广告软件，和其它可能不想安装的应用程序的计划扫描，来实现。请参见 扫描广告软件和可能不想安装的应用程序（第83页）。

如果该应用程序还是不能够被完全检测到，则可能是因为:

- 您的访问权限不足。
- 计算机中的某些包含着该应用程序组件的驱动器，或文件夹，被排除在了扫描之外。

如果是后一种情况，请检查从扫描中排除的项目的列表（参见从读写扫描中排除项目（第86页））。如果有项目出现在列表中，请从列表中删除这些项目，然后，再次扫描您的计算机。

Sophos Endpoint Security and Control 可能不能够彻底检测到或者删除，有组件安装在网络驱动器上的广告软件和其它可能不想安装的应用程序。.

要寻求建议，请联系 Sophos 技术支持。

32.17 频繁发出有关可能不想安装的应用程序的警报

您可能会收到大量的有关可能不想安装的应用程序的警报，包括对同一个应用程序发出多重报告。

出现这种情况的原因是，某些类型的可能不想安装的应用程序会“监控”文件，试图频繁地访问各种文件。如果您启用了读写扫描，Sophos Endpoint Security and Control 则会检测每一个文件的访问，并因此发出警报。

您应该按照以下说明做:

- 禁用针对广告软件和可能不想安装的应用程序的读写扫描。您可以使用计划扫描来替代。
- 批准使用应用程序（假如您想要在计算机上运行该应用程序）。请参见批准广告软件和可能不想安装的应用程序（第84页）。
- 清除计算机，删除您没有批准的应用程序。请参见立即清除计算机（第54页）。

32.18 清除失败

如果 Sophos Endpoint Security and Control 清除项目失败（“清除失败”），原因可能如下:

- 它没有找到多组件项目中的所有组件。请对计算机运行一次完整系统扫描，以找到其它组件。请参见现在扫描计算机（第62页）。
- 某些包含着项目组件的驱动器，或文件夹，被排除在了扫描之外。检查是否有项目被排除在了扫描之外（参见从读写扫描中排除项目（第86页））。如果有项目出现在列表中，请从列表中删除这些项目。

- 您的访问权限不足。
- 它无法清除该类型的项目。
- 它发现的是病毒碎片，而非确切的病毒。
- 该项目在写保护的软盘上，或者在光盘上。
- 该项目在写保护的 NTFS 卷上（Windows 2000 或以后）。

32.19 弥补病毒造成的破坏

清除可以将病毒从计算机中删除，但并不总是能够弥补病毒所造成的破坏。

有些病毒并不会造成破坏。另一些病毒则可能以各种方式更改或损毁数据，并且令人难以觉察。要处理这种情况，您应该:

- 在 **帮助** 菜单中，单击 **查看项目信息**。您将会被连接到 Sophos 网站中，您可以在那里阅读病毒分析。
- 使用备份的，或者原始的程序拷贝，替换被感染过的程序。如果您之前没有做这样的备份，请立即制作或获取一份，以备将来遭到病毒感染时之需。

有时，您可以从被病毒损坏的磁盘上恢复数据。Sophos 可以提供一些工具软件，修复某些病毒造成的损害。请联系Sophos 技术支持寻求建议。

32.20 弥补可能不想安装的应用程序造成的破坏

清除可以将不想安装的应用程序删除，但并不总是能够弥补应用程序所造成的破坏。

有些应用程序会更改操作系统的设置，如：更改您的因特网的连接设置。Sophos Endpoint Security and Control 无法还原所有的设置。例如，某应用程序更改了浏览器的主页，而 Sophos Endpoint Security and Control 不可能知道之前所设置的浏览器主页是什么。

有些应用程序会安装一些实用程序，如：.dll或.ocx文件等，到您的计算机上。如果某个实用程序是无害的（也就是说，它不具有可能不想安装的应用程序的那些特点），如：某个语言库，并且不是不想安装的应用程序中不可缺少的部分，那么，Sophos Endpoint Security and Control 可能不会将其检测为不想安装的应用程序的一部分。在这种情况下，清除将不会从您的计算机中将文件删除。

有时某个应用程序，如：广告软件，是您打算安装的软件中的一部分，并且是运行该程序所要求的。如果您删除了该应用程序，则该软件会停止在您的计算机上运行。

您应该:

- 在 **帮助** 菜单中，单击 **查看项目信息**。 您将会被连接到 Sophos 网站中，您可以在那里阅读应用程序分析。
- 使用备份恢复您的系统设置，或者您所安装的软件。 如果您之前没有做这样的备份，请立即制作一份，以备将来之需。

要了解更多的有关弥补广告软件和可能不想安装的应用程序造成的破坏的信息或建议，请联系 Sophos 技术支持。

32.21 数据控制不能检查通过嵌入式浏览器上传的文件

数据控制会介入通过独立使用的网页浏览器上传的文件。但它不会介入通过嵌入第三方应用程序（如：Lotus Notes）中浏览器上传的文件。 如果您具有带有嵌入式浏览器的第三方应用程序，并且想要监控所有上传的文件，那么，您需要配置该应用程序启动外部的浏览器。

32.22 卸载了的更新管理器出现在控制台中

在您卸载了附加的更新管理器之后，它可能仍然出现在 Enterprise Console 的 **更新管理器** 视图中。

要从控制台中删除更新管理器，请选择它，单击鼠标右键，然后单击 **删除**。

33 用语表

Active Directory 同步化事件 (Active Directory synchroization event)
与 Active Directory 进行同步化时发生的事件。

活动子领域 (active sub-estate)
在组窗格板中显示的子领域。

高级内容控制列表编辑器 (advanced Content Control List editor)
一种编辑器，它使用户能够创建，由积分 (score)，最大计数 (maximum count)，正则表达式 (regular expression)，以及在匹配内容控制列表 (Content Control List) 之前必须达到的触发积分 (trigger score) 等，构成的一种自定义内容控制列表 (custom Content Control List)。

应用程序管理器 (Application manager)
一个对话框，它使您能够，针对被 Sophos Client Firewall 阻断的应用程序，允许或创建新规则。

自动保护 (automatic protection)	一旦安全软件完成了与 Enterprise Console 进行的同步化，就立即将安全软件部署（安装和策略强制实施）到某个 Active Directory 容器中的所有的计算机上。
种类 (category)	一种指定的标记，它用于根据类型 (type)，定义内容的正则 (regulation)，或所应用于的范围 (region)，来分类 SophosLabs 内容控制列表。
内容控制列表 (CCL) (Content Control List (CCL))	指定文件内容的一组条件，例如，与其它形式的个人识别信息在一起的信用卡或借记卡号码，或银行帐号详情。有两种类型的内容控制列表：SophosLabs 内容控制列表，和自定义内容控制列表。
内容规则 (content rule)	一种规则，它包括一个或多个内容控制列表，并指定，如果用户试图传输匹配了规则中的全部内容控制列表的数据到指定目标路径 (destination) 时，采取的措施。
受控程序 (controlled application)	公司想要检测或阻断的非恶意的应用程序，因为它们会影响工作或网络的运行效率。
受控数据 (controlled data)	满足数据控制条件的文件。
受控设备 (controlled device)	受到设备控制功能影响的设备。
紧要级 (critical level)	触发某个项目的安全状态转变为“紧要 (Critical)”的值。
自定义内容控制列表 (custom Content Control List)	由 Sophos 用户创建的内容控制列表。有两种创建自定义内容列表的方式：创建带有特定的搜索条件（如：“所有这些搜索词”）的搜索词的简单列表；或者，使用高级内容控制列表编辑器。
指标面板	网络安全状态的一览图。
指标面板事件 (Dashboard event)	指标面板中的健康指标超过紧要级的事件。在指标面板事件发生时，会发出电子邮件警报。
数据控制	一种功能，用于减少从工作站计算机中意外丢失数据的机会。当工作站计算机的用户试图传输的文件，满足在数据控制策略和规则中定义的标准时，数据控制功能会采取相应的措施。例如，当某用户

	试图复制包含客户资料列表的电子表格文件到可移动的存储设备中时，或者，上传标记为机密的文档到 Webmail 帐户中时，数据控制功能会阻断此传输，如果事先的配置要求这样做。
数据库 (database)	Sophos Enterprise Console 组件，存储有关网络中的计算机的详情。
默认子领域 (Default sub-estate)	目录树的根在服务器的组树的根节点和 **未指派** 组中的子领域。当首次打开 Enterprise Console 时，它会作为默认值显示。
设备控制	一种功能，用于减少从工作站计算机中意外丢失数据的机会，并且可以限制从网络外部引进和安装软件。当工作站计算机用户试图在他们的计算机上，使用某个未经批准的存储设备或网络设备时，该功能会采取措施。
领域 (estate)	请参见 IT estate（IT 领域）的定义。
免除设备 (exempt device)	明确地从设备控制中排除的设备。
表达式 (expression)	参见正则表达式 (regular expression) 的定义。
文件匹配规则 (file matching rule)	一种规则，用于指定，如果用户试图传输带有特定的文件名或特定的文件类型的文件到特定的目标路径 (destination) 时，将要采取的措施，例如，阻断传输数据库到可移动的存储设备中。
组 (group)	在 Sophos Enterprise Console 中定义的受管理的计算机的组。
健康指标 (health indicator)	描述指标面板中某个部分或项目的安全状态，或者，描述网络的总体健康状态的，各种图标的总称。
IT 领域 (IT estate)	公司的 IT 环境，包括计算机，网络，等等。
遗留的更新策略 (legacy updating policy)	在将 Sophos Enterprise Console 从版本 3.x 升级到版本 4.0 之前，已经存在的更新策略。并且这些更新策略在升级之后仍然被使用，直到新的更新策略被应用到一个或多个组中。

受管理的计算机 (managed computer)	安装了远程管理系统(RMS)的计算机，在该计算机上 Sophos Enterprise Console 可以报告，以及安装和更新软件。
管理控制台 (management console)	Sophos Enterprise Console 组件，使您能够保护和管理计算机。
管理服务器 (management server)	Sophos Enterprise Console 组件，处理更新和联网计算机之间的通讯。
最大计数 (maximum count)	可以计入到总积分中的，某正则表达式的匹配数目的最大值。
未及时更新的计算机 (out-of-date computer)	没有及时更新 Sophos 软件的计算机。
策略 (policy)	一组设置，例如：应用到某个组或多个组的计算机上的用于更新的一组设置。
数量 (quantity)	在内容控制列表被匹配之前，必须在文件中找到的内容控制列表的键数据类型 (key data type) 的数量。
数量键 (quantity key)	在内容控制列表中定义的键数据类型 (key type of data)，数量设置将应用于该键数据类型。例如，对于某个包含信用卡或借记卡的号码的内容控制列表，数量指定，在内容控制列表被匹配之前，必须在文件中找到多少信用卡或借记卡的号码。
范围 (region)	SophosLabs 内容控制列表的范围。范围，要么指定内容控制列表（国家特定的内容控制列表）所应用的国家，要么显示为“全球”（应用于所有国家的全球内容控制列表）。
正则表达式 (regular expression)	一种搜索字符串，它使用指定的字符去匹配文件中的文本范式 (text pattern)。数据控制 (Data Control) 使用的是 Perl 5 正则表达式句法 (regular expression syntax)。
权限 (right)	在 Enterprise Console 中执行某种任务的许可的集合。
角色 (role)	决定访问 Enterprise Console 的权限的集合。
基于角色的管理 (role-based administration)	一种功能，它允许根据用户在公司中的角色，指定他们可以访问哪些计算机，以及可以执行哪些任务。

规则	规则，用于指定如果某个文件满足了特定的条件时，所要采取的措施。有两种类型的数据控制规则：文件匹配规则 和 内容规则。
积分 (score)	当某个正则表达式被匹配时，加入到内容控制列表的总积分 (total score) 中的分数。
服务器根节点 (server root node)	在 **组** 窗格板中的组树中的最高层的节点，它包括 **未指派** 组。
Sophos Enterprise Console	用于安装和管理联网计算机上的 Sophos 产品的软件。
Sophos Live Protection	一种使用云计算技术的功能，它能不断地判断可疑文件是否成为安全隐患，并随时采取在 Sophos 防病毒保护配置中所指定的相应措施。
Sophos Update Manager (SUM)	一种程序，用于将 Sophos 安全软件和更新文件从 Sophos或其它更新服务器上下载到共享的更新路径中。
Sophos 定义规则 (Sophos-defined rule)	由 Sophos 提供的作为范例的规则。Sophos 不更新 Sophos 定义规则。
SophosLabs 内容控制列表 (SophosLabs Content Control List)	由Sophos提供和管理的一种内容控制列表。Sophos 可以更新 SophosLabs 内容控制列表，或创建新的内容控制列表，并在 Enterprise Console 中提供这些列表。SophosLabs 内容控制列表中的内容无法被编辑。不过，可以为每个这样的内容控制列表设置数量 (quantity)。
子领域 (sub-estate)	IT 领域中某命名部分，包括计算机和组的子网。
子领域管理 (sub-estate administration)	一种功能，它可以限制在某些计算机和组上执行某些操作。
软件预订 (software subscription)	针对各种操作平台的各种软件集，由用户选择后，更新管理器会下载它们，并保持更新它们。一个版本可以被指定为针对各个受支持的操作平台（例如：为 Windows 2000 及以后指定“最新”）。
同步化间隔 (synchronization interval)	在 Enterprise Console 中同步化点与所选的 Active Directory容器进行了同步化之后，到下一次进行同步化之间的时间间隔。

(针对 Active Directory 树的) 同步化点 (synchronization point (for an Active Directory tree))	一个 Sophos Enterprise Console 组，在该组中，所选的 Active Directory 容器（组和计算机，或者，只有组）里的内容，会被添加以进行同步化，它们的结构会保留不变。
与 Active Directory 同步化	Sophos Enterprise Console 组与 Active Directory 组织单元 (organizational unit)，或者容器进行的单向同步化。
已同步化的组	在同步化点下的任何组。
系统管理员 (System Administrator)	预置角色，具有管理网络中的 Sophos 安全软件，以及管理 Enterprise Console 中的角色的所有权限。 系统管理员 (System Administrator) 角色不能被删除，也不被更改名称或权限，并且 Sophos Full Administrators Windows 组不能从中被删除。其它的用户和组可以在角色中被添加或删除。
标记 (tag)	应用到 SophosLabs 内容控制列表中的一种标识符 (descriptor)，以识别内容控制列表的内容或范围。有三种类型的标记：类型 (type)，正则 (regulation)，以及范围 (region)。
介入防范	能够防范已知的恶意软件，以及防止未经授权的用户通过 Sophos Endpoint Security and Control 用户界面，卸载或禁用 Sophos 安全软件的一种功能。
指标级别 (threshold level)	触发某个项目的安全状态转变为“提醒 (Warning)”或“紧要 (Critical)”的值。
总积分 (total score)	按照已被满足的内容，某个内容控制列表所计的总积分。
触发积分 (trigger score)	在内容控制列表被匹配之前，正则表达式必须被匹配的次数。
真实文件类型 (true file type)	经过分析文件的结构，而不是通过文件的文件扩展名，而确认的文件类型。这是一种更加可靠的确认文件类型的方法。
类型 (type)	SophosLabs 内容控制列表分类所依据的标准，例如，某个内容控制列表定义的护照详情，邮寄地

	址，或者，电子邮件地址，属于个人识别信息类型 (Personally Identifiable Information type)。
更新管理器	参见 Sophos Update Manager 的定义。
提醒级 (warning level)	触发某个项目的安全状态转变为 “提醒 (Warning)” 的值。

34 技术支持

您可以通过以下各种方式获得 Sophos 产品的技术支持:

- 访问 *http://community.sophos.com/* 的 SophosTalk 论坛，并搜索遇到相同问题的其它用户。
- 访问*http://www.sophos.com/support/* 的 Sophos 技术支持知识库。
- 在 *http://www.sophos.com/support/docs/* 中下载产品的技术文档。
- 发送电子邮件至: *support@sophos.com*，提供您的 Sophos 软件的版本号，计算机的操作系统，补丁级别，以及任何出错信息的原文。

35 法律声明

ACE™, TAO™, CIAO™, and CoSMIC™

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software.Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model.You needn’ t inform anyone that you’ re using DOC software in your software, though we encourage you to let us[11] know so we can promote your project in the DOC software success stories[12].

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice.Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement.A number of companies[13] around the world provide commercial support for DOC software, however.DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof.Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE[14], TAO[15], CIAO[16], and CoSMIC[17] web sites are maintained by the DOC Group[18] at the Institute for Software Integrated Systems (ISIS)[19] and the Center for Distributed Object Computing of Washington University, St. Louis[20] for the development of open-source software as part of the open-source software community[21].By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership.In addition, submitters acknowledgethat any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software.By making a submission, submitter agree to these terms.Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, WashingtonUniversity, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University.Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me[22] know.

Douglas C. Schmidt[23]

References

1. http://www.cs.wustl.edu/~schmidt/ACE.html
2. http://www.cs.wustl.edu/~schmidt/TAO.html
3. http://www.dre.vanderbilt.edu/CIAO/
4. http://www.dre.vanderbilt.edu/cosmic/
5. http://www.dre.vanderbilt.edu/~schmidt/
6. http://www.cs.wustl.edu/~schmidt/ACE-members.html
7. http://www.wustl.edu/
8. http://www.uci.edu/
9. http://www.vanderbilt.edu/
10. http://www.the-it-resource.com/Open-Source/Licenses.html
11. mailto:doc_group@cs.wustl.edu
12. http://www.cs.wustl.edu/~schmidt/ACE-users.html
13. http://www.cs.wustl.edu/~schmidt/TAO.html
14. http://www.cs.wustl.edu/~schmidt/ACE.html
15. http://www.cs.wustl.edu/~schmidt/TAO.html
16. http://www.dre.vanderbilt.edu/CIAO/
17. http://www.dre.vanderbilt.edu/cosmic/
18. http://www.dre.vanderbilt.edu
19. http://www.isis.vanderbilt.edu/
20. http://www.cs.wustl.edu/~schmidt/doc-center.html
21. http://www.opensource.org/
22. mailto:d.schmidt@vanderbilt.edu
23. http://www.dre.vanderbilt.edu/~schmidt/

Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License.A copy of the license agreement for any such included software can be found at *http://www.apache.org/licenses/LICENSE-2.0*.

Common Public License

The Sophos software that is described in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code.The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form.For any such software covered under the CPL, the source code is available via mail order by submitting a

request to Sophos; via email to *support@sophos.com* or via the web at *http://www.sophos.com/support/queries/enterprise.html*.A copy of the license agreement for any such included software can be found at *http://opensource.org/licenses/cpl1.0.php*

iMatix SFL

This product uses parts of the iMatix SFL, Copyright © 1991-2000 iMatix Corporation *http://www.imatix.com*.

OpenSSL cryptographic toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.See below for the actual license texts.Actually both licenses are BSD-style Open Source licenses.In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998 2006 The OpenSSL Project.All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.(http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission.For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,

INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).The implementation was written so as to conform with Netscape’ s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to.The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code.The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’ s, and as such any Copyright notices in the code are not to be removed.If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

   The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

索引

字母

A

B

C

D

F

K

L

M

P

Q

R

S

X

Y

Z